Cisco Unified IP Phone 7970G/7971G-GE Administration Guide for Cisco Unified Communications Manager 7.0 (SCCP and SIP)

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-15299-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

The Java logo is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries.

Cisco Unified IP Phone 7970G/7971G-GE Administration Guide for Cisco Unified Communications Manager 7.0
© 2008 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xi

Overview xi

Audience xi

Organization xi

Related Documentation xii

Obtaining Documentation, Obtaining Support, and Security Guidelines xiii

Cisco Product Security Overview xiii

Document Conventions xiii

CHAPTER 1 **An Overview of the Cisco Unified IP Phone** 1-1

Understanding the Cisco Unified IP Phone 7970 Series 1-1

What Networking Protocols Are Used? 1-3

What Features are Supported on the Cisco Unified IP Phone 7970 Series? 1-7

Feature Overview 1-7

Configuring Telephony Features 1-8

Configuring Network Parameters Using the Cisco Unified IP Phone 1-8

Providing Users with Feature Information 1-8

Understanding Security Features for Cisco Unified IP Phones 1-8

Overview of Supported Security Features 1-10

Understanding Security Profiles 1-12

Identifying Authenticated, Encrypted, and Protected Phone Calls 1-13

Establishing and Identifying Secure Conference Calls 1-14

Establishing and Identifying Protected Calls 1-14

Call Security Interactions and Restrictions 1-15

Supporting 802.1X Authentication on Cisco Unified IP Phones 1-16

Overview 1-16

Required Network Components 1-16

Best Practices—Requirements and Recommendations 1-17

Security Restrictions 1-17

Overview of Configuring and Installing Cisco Unified IP Phones 1-18

Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager 1-18

Checklist for Configuring the Cisco Unified IP Phone 7970 Series in Cisco Unified Communications Manager 1-19

Installing Cisco Unified IP Phones 1-21
Checklist for Installing the Cisco Unified IP Phone 7970 Series 1-21

CHAPTER 2 **Preparing to Install the Cisco Unified IP Phone on Your Network** 2-1

Understanding Interactions with Other Cisco Unified IP Communications Products 2-2
Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager 2-2
Understanding How the Cisco Unified IP Phone Interacts with the VLAN 2-3
Providing Power to the Phone 2-3
Power Guidelines 2-4
Phone Power Consumption and Display Brightness 2-5
Power Outage 2-5
Obtaining Additional Information about Power 2-6
Understanding Phone Configuration Files 2-6
Understanding the Phone Startup Process 2-7
Adding Phones to the Cisco Unified Communications Manager Database 2-9
Adding Phones with Auto-Registration 2-10
Adding Phones with Auto-Registration and TAPS 2-11
Adding Phones with Cisco Unified Communications Manager Administration 2-12
Adding Phones with BAT 2-12
Using Cisco Unified IP Phones with Different Protocols 2-12
Converting a New Phone from SCCP to SIP 2-13
Converting an In-Use Phone from SCCP to SIP 2-13
Converting an In-Use Phone from SIP to SCCP 2-13
Deploying a Phone in an SCCP and SIP Environment 2-14
Determining the MAC Address of a Cisco Unified IP Phone 2-14

CHAPTER 3 **Setting Up the Cisco Unified IP Phone** 3-1

Before You Begin 3-1
Network Requirements 3-1
Cisco Unified Communications Manager Configuration 3-2
Understanding the Cisco Unified IP Phone 7970 Series Components 3-2
Network and Access Ports 3-2
Handset 3-3
Speakerphone 3-3
Headset 3-3
Audio Quality Subjective to the User 3-4
Connecting a Headset 3-4

Disabling a Headset 3-4
Using External Devices 3-4
Installing the Cisco Unified IP Phone 3-5
Attaching the Cisco Unified IP Phone Expansion Module 7914 3-7
Adjusting the Placement of the Cisco Unified IP Phone 3-8
Adjusting Cisco Unified IP Phone Footstand and Phone Height 3-8
Securing the Phone with a Cable Lock 3-8
Mounting the Phone to the Wall 3-9
Verifying the Phone Startup Process 3-10
Configuring Startup Network Settings 3-11
Configuring Security on the Cisco Unified IP Phone 3-12

CHAPTER 4 **Configuring Settings on the Cisco Unified IP Phone 4-1**
Configuration Menus on the Cisco Unified IP Phone 7970 Series 4-1
Displaying a Configuration Menu 4-2
Unlocking and Locking Options 4-3
Editing Values 4-3
Overview of Options Configurable from a Phone 4-4
Network Configuration Menu 4-5
Device Configuration Menu 4-10
Unified CM Configuration 4-11
SIP Configuration Menu (SIP Phones Only) 4-12
SIP General Configuration Menu 4-13
Line Settings Menu (SIP Phones Only) 4-14
Call Preferences Menu (SIP Phones Only) 4-14
HTTP Configuration Menu 4-15
Locale Configuration Menu 4-16
NTP Configuration Menu (SIP Phones Only) 4-17
UI Configuration Menu 4-17
Media Configuration Menu 4-19
Power Save Configuration Menu 4-22
Ethernet Configuration Menu 4-23
Security Configuration Menu 4-23
QoS Configuration Menu 4-25
Network Configuration 4-25
Security Configuration Menu 4-29
CTL File Menu 4-30

Trust List Menu 4-31
802.1X Authentication and Status 4-31

CHAPTER 5 **Configuring Features, Templates, Services, and Users 5-1**
Telephony Features Available for the Phone 5-1
Configuring Corporate and Personal Directories 5-16
Configuring Corporate Directories 5-17
Configuring Personal Directory 5-17
Modifying Phone Button Templates 5-17
Modifying a Phone Button Template for Personal Address Book or Fast Dials 5-18
Configuring Softkey Templates 5-19
Setting Up Services 5-20
Adding Users to Cisco Unified Communications Manager 5-20
Managing the User Options Web Pages 5-21
Giving Users Access to the User Options Web Pages 5-21
Specifying Options that Appear on the User Options Web Pages 5-21

CHAPTER 6 **Customizing the Cisco Unified IP Phone 6-1**
Customizing and Modifying Configuration Files 6-1
Creating Custom Phone Rings 6-2
Ringlist.xml File Format Requirements 6-2
PCM File Requirements for Custom Ring Types 6-3
Configuring a Custom Phone Ring 6-3
Creating Custom Background Images 6-3
List.xml File Format Requirements 6-4
PNG File Requirements for Custom Background Images 6-5
Configuring a Custom Background Image 6-5
Configuring Wideband Codec 6-6
Configuring the Idle Display 6-7
Automatically Disabling the Cisco Unified IP Phone Touchscreen 6-7

CHAPTER 7 **Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone 7-1**
Model Information Screen 7-2
Status Menu 7-3
Status Messages Screen 7-3
Network Statistics Screen 7-9
Firmware Versions Screen 7-11

Expansion Module(s) Screen 7-12
Call Statistics Screen 7-13

CHAPTER 8 **Monitoring the Cisco Unified IP Phone Remotely** 8-1
Accessing the Web Page for a Phone 8-1
Disabling and Enabling Web Page Access 8-3
Device Information 8-3
Network Configuration 8-4
Network Statistics 8-8
Device Logs 8-10
Streaming Statistics 8-10

CHAPTER 9 **Troubleshooting and Maintenance** 9-1
Resolving Startup Problems 9-1
Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process 9-2
Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager 9-2
Identifying Error Messages 9-3
Checking Network Connectivity 9-3
Verifying TFTP Server Settings 9-3
Verifying IP Addressing and Routing 9-3
Verifying DNS Settings 9-4
Verifying Cisco Unified Communications Manager Settings 9-4
Cisco CallManager and TFTP Services Are Not Running 9-4
Creating a New Configuration File 9-5
Registering the Phone with Cisco Unified Communications Manager 9-5
Symptom: Cisco Unified IP Phone Unable to Obtain IP Address 9-6
Cisco Unified IP Phone Resets Unexpectedly 9-6
Verifying Physical Connection 9-6
Identifying Intermittent Network Outages 9-6
Verifying DHCP Settings 9-7
Checking Static IP Address Settings 9-7
Verifying Voice VLAN Configuration 9-7
Verifying that the Phones Have Not Been Intentionally Reset 9-7
Eliminating DNS or Other Connectivity Errors 9-7
Checking Power Connection 9-8
Troubleshooting Cisco Unified IP Phone Security 9-8
General Troubleshooting Tips 9-10

General Troubleshooting Tips for the Cisco Unified IP Phone Expansion Module 7914 9-12
Resetting or Restoring the Cisco Unified IP Phone 9-13
Performing a Basic Reset 9-13
Performing a Factory Reset 9-14
Using the Quality Report Tool 9-14
Monitoring the Voice Quality of Calls 9-15
Using Voice Quality Metrics 9-15
Troubleshooting Tips 9-16
Where to Go for More Troubleshooting Information 9-17
Cleaning the Cisco Unified IP Phone 9-17

APPENDIX A **Providing Information to Users Via a Website** A-1
How Users Obtain Support for the Cisco Unified IP Phone A-1
Giving Users Access to the User Options Web Pages A-1
How Users Access the Online Help System on the Phone A-2
How Users Get Copies of Cisco Unified IP Phone Manuals A-2
Accessing Cisco 7900 Series Unified IP Phone eLearning Tutorials (SCCP Phones Only) A-2
How Users Subscribe to Services and Configure Phone Features A-3
How Users Access a Voice-Messaging System A-3
How Users Configure Personal Directory Entries A-4
Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer A-4

APPENDIX B **Feature Support by Protocol for the Cisco Unified IP Phones 7970 Series** B-1

APPENDIX C **Supporting International Users** C-1
Adding Language Overlays to Phone Buttons C-1
Installing the Cisco Unified Communications Manager Locale Installer C-1
Support for International Call Logging C-2

APPENDIX D **Technical Specifications** D-1
Physical and Operating Environment Specifications D-1
Cable Specifications D-2
Network and Access Port Pinouts D-2

APPENDIX E **Basic Phone Administration Steps** E-1
Example User Information for these Procedures E-1

Adding a User to Cisco Unified Communications Manager E-2
Adding a User From an External LDAP Directory E-2
Adding a User Directly to Cisco Unified Communications Manager E-2
Configuring the Phone E-3
Performing Final End User Configuration Steps E-7

INDEX

Preface

Overview

Cisco Unified IP Phone 7970G/7971G-GE Administration Guide for Cisco Unified Communications Manager 7.0 provides the information you need to understand, install, configure, manage, and troubleshoot the phones in the Cisco Unified IP Phone 7970 series on a Voice-over-IP (VoIP) network.

Because of the complexity of a Unified Communications network, this guide does not provide complete and detailed information for procedures that you need to perform in Cisco Unified Communications Manager (formerly Cisco Unified CallManager) or other network devices. See the "Related Documentation" section on page xii for a list of related documentation.

Audience

Network engineers, system administrators, or telecom engineers should review this guide to learn the steps required to properly set up the Cisco Unified IP Phone 7970 Series on the network.

The tasks described are administration-level tasks and are not intended for end-users of the phones. Many of the tasks involve configuring network settings and affect the phone's ability to function in the network.

Because of the close interaction between the Cisco Unified IP Phone and Cisco Unified Communications Manager, many of the tasks in this manual require familiarity with Cisco Unified Communications Manager.

Organization

This manual is organized as follows:

Chapter 1, "An Overview of the Cisco Unified IP Phone"	Provides a conceptual overview and description of the Cisco Unified IP Phone
Chapter 2, "Preparing to Install the Cisco Unified IP Phone on Your Network"	Describes how the Cisco Unified IP Phone interacts with other key IP telephony components, and provides an overview of the tasks required prior to installation
Chapter 3, "Setting Up the Cisco Unified IP Phone"	Describes how to properly and safely install and configure the Cisco Unified IP Phone on your network

Chapter 4, “Configuring Settings on the Cisco Unified IP Phone”	Describes how to configure network settings, verify status, and make global changes to the Cisco Unified IP Phone
Chapter 5, “Configuring Features, Templates, Services, and Users”	Provides an overview of procedures for configuring telephony features, configuring directories, configuring phone button and softkey templates, setting up services, and adding users to Cisco Unified Communications Manager
Chapter 6, “Customizing the Cisco Unified IP Phone”	Explains how to customize phone ring sounds, background images, and the phone idle display at your site
Chapter 7, “Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone”	Explains how to view model information, status messages, network statistics, and firmware information from the Cisco Unified IP Phone
Chapter 8, “Monitoring the Cisco Unified IP Phone Remotely”	Describes the information that you can obtain from the phone’s web page, and how to use this information to remotely monitor the operation of a phone and to assist with troubleshooting
Chapter 9, “Troubleshooting and Maintenance”	Provides tips for troubleshooting the Cisco Unified IP Phone
Appendix A, “Providing Information to Users Via a Website”	Provides suggestions for setting up a website for providing users with important information about their Cisco Unified IP Phones
Appendix B, “Feature Support by Protocol for the Cisco Unified IP Phones 7970 Series”	Provides information about feature support for the Cisco Unified IP Phone using the SCCP or SIP protocol
Appendix C, “Supporting International Users”	Provides information about setting up phones in non-English environments
Appendix D, “Technical Specifications”	Provides technical specifications of the Cisco Unified IP Phone
Appendix E, “Basic Phone Administration Steps”	Provides procedures for basic administration tasks such as adding a user and phone to Cisco Unified Communications Manager and then associating the user to the phone.

Related Documentation

For more information about Cisco Unified IP Phones or Cisco Unified Communications Manager, refer to the following publications:

Cisco Unified IP Phone 7970 Series

These publications are available at the following URL:

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

- *Cisco Unified IP Phone 7970 Series Phone Guide*
- *Cisco Unified IP Phone Features A–Z*
- *Cisco Unified IP Phone Expansion Module 7914 Phone Guide*
- *Installing the Wall Mount Kit for the Cisco Unified IP Phone*
- *Regulatory Compliance and Safety Information for the Cisco Unified IP Phones*
- *Open Source License Notices for the Cisco Unified IP Phones 7900 Series*

Cisco Unified Communications Manager Administration

These publications are available at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Cisco Unified Communications Manager Business Edition

These publications are available at the following URL:

http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.

Convention	Description
boldface screen font	Information you must enter is in **boldface screen** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.**

CHAPTER 1

An Overview of the Cisco Unified IP Phone

The Cisco Unified IP Phone 7970 Series are full-featured telephones that provide voice communication over an Internet Protocol (IP) network. They function much like digital business phones, allowing you to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because Cisco Unified IP Phones are connected to your data network, they offer enhanced IP telephony features, including access to network information and services, and customizeable features and services. The phones also support security features that include file authentication, device authentication, signaling encryption, and media encryption.

The Cisco Unified IP Phone 7970 Series provides a color touchscreen, support for up to eight line or speed dial numbers, context-sensitive online help for buttons and features, and a variety of other sophisticated functions.

The Cisco Unified IP Phone, like other network devices, must be configured and managed. These phones encodes G.711a, G.711µ, G.722, G.729a, G.729ab, iLBC, and decode G.711a, G.711µ, G722, iLBC, and G.729, G729a, G.729b, and G.729ab. These phones also support uncompressed wideband (16bits, 16kHz) audio.

This chapter includes the following topics:

- Understanding the Cisco Unified IP Phone 7970 Series, page 1-1
- What Networking Protocols Are Used?, page 1-3
- What Features are Supported on the Cisco Unified IP Phone 7970 Series?, page 1-7
- Understanding Security Features for Cisco Unified IP Phones, page 1-8
- Overview of Configuring and Installing Cisco Unified IP Phones, page 1-18

Caution Using a cell, mobile, or GSM phone, or two-way radio in close proximity to a Cisco Unified IP Phone might cause interference. For more information, refer to the manufacturer documentation of the interfering device.

Understanding the Cisco Unified IP Phone 7970 Series

Figure 1-1 shows the main components of the Cisco Unified IP Phone 7970 Series.

Figure 1-1 Cisco Unified IP Phone

1	Programmable buttons	Depending on configuration, programmable buttons provide access to: • Phone lines (line buttons) • Speed-dial numbers (speed-dial buttons, including the BLF speed-dial feature) • Web-based services (for example, a Personal Address Book button) • Phone features (for example, a Privacy button) Buttons illuminate to indicate status: Green, steady—Active call Green, flashing—Held call Amber, steady—Privacy in use Amber, flashing—Incoming call Red, steady—Remote line in use (shared line or BLF status)
2	Footstand adjustment button	Allows you to adjust the angle of the phone base.
3	Display button	Awakens the touchscreen from sleep mode or disables it for cleaning. No color—Ready for input Green flashing—Disabled Green steady—Sleep mode
4	Messages button	Auto-dials your voice message service (varies by service).

5	Directories button	Opens/closes the Directories menu. Use it to access call logs and directories.
6	Help button	Activates the Help menu.
7	Settings button	Opens/closes the Settings menu. Use it to change touchscreen and ring settings.
8	Services button	Opens/closes the Services menu.
9	Volume button	Controls the handset, headset, and speakerphone volume (off-hook) and the ringer volume (on-hook).
10	Speaker button	Toggles the speakerphone on or off.
11	Mute button	Toggles the Mute feature on or off.
12	Headset button	Toggles the headset on or off.
13	Navigation button	Allows you to scroll through menus and highlight items. When the phone is on-hook, displays phone numbers from your Placed Calls log.
14	Keypad	Allows you to dial phone numbers, enter letters, and choose menu items.
15	Softkey buttons	Each activates a softkey option (displayed on your touchscreen).
16	Handset light strip	Indicates an incoming call or new voice message.
17	Touchscreen	Shows phone features.

What Networking Protocols Are Used?

Cisco Unified IP Phones support several industry-standard and Cisco networking protocols required for voice communication. Table 1-1 provides an overview of the networking protocols that the Cisco Unified IP Phone 7970 Series supports.

Table 1-1 Supported Networking Protocols on the Cisco Unified IP Phone

Networking Protocol	Purpose	Usage Notes
Bootstrap Protocol (BootP)	BootP enables a network device such as the Cisco Unified IP Phone to discover certain startup information, such as its IP address.	If you are using BootP to assign IP addresses to the Cisco Unified IP Phone, the BOOTP Server option shows "Yes" in the network configuration settings on the phone.
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP is a Cisco proprietary protocol used to form a-peer-to-peer hierarchy of devices. CPPDP is also used to copy firmware or other files from peer devices to neighboring devices.	CPPDP is used by the Peer Firmware Sharing feature.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and have the phone become operational without needing to manually assign an IP address or configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional information about DHCP configurations, refer to the "Cisco TFTP" chapter in *Cisco Unified Communications Manager System Guide*.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for the XML services and for troubleshooting purposes.
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.	The Cisco Unified IP Phone implements the IEEE 802.1X standard by providing support for the EAP-MD5 option for 802.1X authentication. When 802.1X authentication is enabled on the phone, you should disable the PC port and voice VLAN. Refer to the "Supporting 802.1X Authentication on Cisco Unified IP Phones" section on page 1-16 for additional information.

Table 1-1 Supported Networking Protocols on the Cisco Unified IP Phone (continued)

Networking Protocol	Purpose	Usage Notes
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.
Link Layer Discovery Protocol (LLDP)	LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.	The Cisco Unified IP Phone supports LLDP on the PC port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voice products.	The Cisco Unified IP Phone supports LLDP-MED on the SW port to communicate information such as: • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED support, see the *LLDP-MED and Cisco Discovery Protocol* white paper: http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
Real-Time Control Protocol (RTCP)	RTCP works with Real-Time Transport Protocol (RTP) to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams.	RTCP is disabled by default, but you can enable it on a per-phone basis using Cisco Unified Communications Manager. For more information, see the "Network Configuration" section on page 4-25.
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.

Table 1-1 Supported Networking Protocols on the Cisco Unified IP Phone (continued)

Networking Protocol	Purpose	Usage Notes
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* provides the ability to control the attributes of an end-to-end call. You can configure the Cisco Unified IP Phone to use either SIP or Skinny Client Control Protocol (SCCP).
Skinny Client Control Protocol (SCCP)	SCCP includes a messaging set that allows communications between call control servers and endpoint clients such as IP Phones. SCCP is proprietary to Cisco Systems.	Cisco Unified IP Phones use SCCP for call control. You can configure the Cisco Unified IP Phone to use either SCCP or Session Initiation Protocol (SIP).
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established using only the SDP capabilities that are supported by all endpoints in the conference.	SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by Cisco Unified Communications Manager or Media Gateway in operation. Some SIP endpoints may allow these parameters to be configured on the endpoint itself.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, Cisco Unified IP Phones use the TLS protocol when securely registering with Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign TFTP server from the Network Configuration menu on the phone.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones transmit and receive RTP streams, which utilize UDP.

Related Topics

- Understanding Interactions with Other Cisco Unified IP Communications Products, page 2-2
- Understanding the Phone Startup Process, page 2-7
- Network Configuration Menu, page 4-5

What Features are Supported on the Cisco Unified IP Phone 7970 Series?

The Cisco Unified IP Phone functions much like a digital business phone, allowing you to place and receive telephone calls. In addition to traditional telephony features, the Cisco Unified IP Phone includes features that enable you to administer and monitor the phone as a network device.

This section includes the following topics:

- Feature Overview, page 1-7
- Configuring Telephony Features, page 1-8
- Configuring Network Parameters Using the Cisco Unified IP Phone, page 1-8
- Providing Users with Feature Information, page 1-8

Feature Overview

Cisco Unified IP Phones provide traditional telephony functionality, such as call forwarding and transferring, redialing, speed dialing, conference calling, and voice messaging system access. Cisco Unified IP phones also provide a variety of other features. For an overview of the telephony features that the Cisco Unified IP Phone supports, see the "Telephony Features Available for the Phone" section on page 5-1.

As with other network devices, you must configure Cisco Unified IP Phones to prepare them to access Cisco Unified Communications Manager and the rest of the IP network. By using DHCP, you have fewer settings to configure on a phone, but if your network requires it, you can manually configure an IP address, TFTP server, subnet information, etc. For instructions on configuring the network settings on the Cisco Unified IP Phones, see Chapter 4, "Configuring Settings on the Cisco Unified IP Phone."

The Cisco Unified IP Phone can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate the Cisco Unified IP Phones with the corporate Lightweight Directory Access Protocol 3 (LDAP3) standard directory to enable users to search for co-workers contact information directly from their IP phones. You can also use XML to enable users to access information such as weather, stocks, quote of the day, and other web-based information. For information about configuring such services, see the "Configuring Corporate Directories" section on page 5-17 and the "Setting Up Services" section on page 5-20.

Finally, because the Cisco Unified IP Phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their IP phones. See Chapter 7, "Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone," for more information.

Related Topics

- Configuring Settings on the Cisco Unified IP Phone, page 4-1
- Configuring Features, Templates, Services, and Users, page 5-1
- Troubleshooting and Maintenance, page 9-1

Configuring Telephony Features

You can modify certain settings for the Cisco Unified IP Phone from the Cisco Unified Communications Manager Administration application. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks. See the "Telephony Features Available for the Phone" section on page 5-1 and *Cisco Unified Communications Manager Administration Guide* for additional information.

For more information about the Cisco Unified Communications Manager Administration application, refer to Cisco Unified Communications Manager documentation, including *Cisco Unified Communications Manager System Guide*. You can also use the context-sensitive help available within the application for guidance.

You can access the complete Cisco Unified Communications Manager documentation suite at this location:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Related Topic

- Telephony Features Available for the Phone, page 5-1

Configuring Network Parameters Using the Cisco Unified IP Phone

You can configure parameters such as DHCP, TFTP, and IP settings on the phone itself. You can also obtain statistics about a current call or firmware versions on the phone.

For more information about configuring features and viewing statistics from the phone, see Chapter 4, "Configuring Settings on the Cisco Unified IP Phone," and see Chapter 7, "Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone."

Providing Users with Feature Information

If you are a system administrator, you are likely the primary source of information for Cisco Unified IP Phone users in your network or company. To ensure that you distribute the most current feature and procedural information, familiarize yourself with Cisco Unified IP Phone documentation. Make sure to visit the Cisco Unified IP Phone web site:

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

From this site, you can access various user guides, including wallet cards.

In addition to providing users with documentation, it is important to inform them about available Cisco Unified IP Phone features—including features specific to your company or network—and about how to access and customize those features, if appropriate.

For a summary of some of the key information that phone users need their system administrators to provide, see Appendix A, "Providing Information to Users Via a Website."

Understanding Security Features for Cisco Unified IP Phones

Implementing security in the Cisco Unified Communications Manager system prevents identity theft of the phone and Cisco Unified Communications Manager server, prevents data tampering, and prevents call signaling and media stream tampering.

To alleviate these threats, the Cisco Unified IP telephony network establishes and maintains authenticated and encrypted communication streams between a phone and the server, digitally signs files before they are transferred to a phone, and encrypts media streams and call signaling between Cisco Unified IP phones.

The Cisco Unified IP Phones Series use the Phone Security Profile, which defines whether the device is nonsecure, authenticated, or encrypted. For information on applying the security profile to the phone, refer to *Cisco Unified Communications Manager Security Guide*.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, refer to the "Configuring Encrypted Phone Configuration Files" chapter in *Cisco Unified Communications Manager Security Guide*.

Table 1-2 shows where you can find additional information about security in this and other documents.

Table 1-2 Cisco Unified IP Phone and Cisco Unified Communications Manager Security Topics

Topic	Reference
Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones	Refer to *Cisco Unified Communications Manager Security Guide*
Security features supported on the Cisco Unified IP Phone	See the "Overview of Supported Security Features" section on page 1-10
Restrictions regarding security features	See the "Security Restrictions" section on page 1-17
Viewing a security profile name	See the "Understanding Security Profiles" section on page 1-12
Identifying phone calls for which security is implemented	See the "Identifying Authenticated, Encrypted, and Protected Phone Calls" section on page 1-13
TLS connection	See the "What Networking Protocols Are Used?" section on page 1-3 See the "Understanding Phone Configuration Files" section on page 2-6
Security and the phone startup process	See the "Understanding the Phone Startup Process" section on page 2-7
Security and phone configuration files	See the "Understanding Phone Configuration Files" section on page 2-6
Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented	See Table 4-2 in the "Network Configuration Menu" section on page 4-5
Understanding security icons in the Unified CM 1 through Unified CM 5 options in the Device Configuration Menu on the phone	See the "Unified CM Configuration" section on page 4-11
Items on the Security Configuration menu that you access from the Device Configuration menu on the phone	See the "Security Configuration Menu" section on page 4-23
Items on the Security Configuration menu that you access from the Settings menu on the phone	See the "Security Configuration Menu" section on page 4-29
Unlocking the CTL file	See the "CTL File Menu" section on page 4-30

Table 1-2 Cisco Unified IP Phone and Cisco Unified Communications Manager Security Topics (continued)

Topic	Reference
Disabling access to web pages for a phone	See the "Disabling and Enabling Web Page Access" section on page 8-3
Troubleshooting	See the "Troubleshooting Cisco Unified IP Phone Security" section on page 9-8 Refer to *Cisco Unified Communications Manager Security Guide,* Troubleshooting chapter
Deleting the CTL file from the phone	See the "Resetting or Restoring the Cisco Unified IP Phone" section on page 9-13
Resetting or restoring the phone	See the "Resetting or Restoring the Cisco Unified IP Phone" section on page 9-13
802.1X Authentication for Cisco Unified IP Phones	See these sections: • "Supporting 802.1X Authentication on Cisco Unified IP Phones" section on page 1-16 • "802.1X Authentication and Status" section on page 4-31 • "Troubleshooting Cisco Unified IP Phone Security" section on page 9-8

Overview of Supported Security Features

Table 1-3 provides an overview of the security features that the Cisco Unified IP Phone 7970 Series supports. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, refer to *Cisco Unified Communications Manager Security Guide*.

For information about current security settings on a phone, look at the Security Configuration menus on the phone (choose **Settings > Security Configuration** and choose **Settings > Device Configuration > Security Configuration**). For more information, see Chapter 4, "Configuring Settings on the Cisco Unified IP Phone."

Note Most security features are available only if a certificate trust list (CTL) is installed on the phone. For more information about the CTL, refer to "Configuring the Cisco CTL Client" chapter in the *Cisco Unified Communications Manager Security Guide*.

Table 1-3 Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sbn) prevent tampering with the firmware image before it is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer-site certificate installation	Each Cisco Unified IP Phone requires a unique certificate for device authentication. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the CAPF (Certificate Authority Proxy Function). Alternatively, you can install an LSC from the Security Configuration menu on the phone. See the "Configuring Security on the Cisco Unified IP Phone" section on page 3-12 for more information.
Device authentication	Occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the phone and a Cisco Unified Communications Manager should occur, and, if necessary, creates a secure signaling path between the entities using TLS protocol. Cisco Unified Communications Manager does not register phones unless they can be authenticated by the Cisco Unified Communications Manager.
File authentication	Validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.
Signaling Authentication	Uses the TLS protocol to validate that no tampering has occurred to signaling packets during transmission.
Manufacturing installed certificate	Each Cisco Unified IP Phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC is a permanent unique proof of identity for the phone, and allows Cisco Unified Communications Manager to authenticate the phone.
Secure SRST reference (SCCP phones only)	After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Media encryption	Uses SRTP to ensure that the media streams between supported devices proves secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.
Signaling encryption (SCCP phones only)	Ensures that all SCCP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and it interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally.

Table 1-3 Overview of Security Features (continued)

Feature	Description
Security profiles	Defines whether the phone is nonsecure, authenticated, encrypted, or protected. See the "Understanding Security Profiles" section on page 1-12 for more information.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional disabling of the web server functionality for a phone	You can prevent access to a phone's web page, which displays a variety of operational statistics for the phone.
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: • Disabling PC port • Disabling Gratuitous ARP (GARP) • Disabling PC Voice VLAN access • Disabling access to the Setting menus, or providing restricted access that allows access to the User Preferences menu and saving volume changes only • Disabling access to web pages for a phone. **Note** You can view current settings for the PC Port Disabled, GARP Enabled, and Voice VLAN enabled options by looking at the phone's Security Configuration menu. For more information, see the "Device Configuration Menu" section on page 4-10.
802.1X Authentication	The Cisco Unified IP Phone can use 802.1X authentication to request and gain access to the network. See the "Supporting 802.1X Authentication on Cisco Unified IP Phones" section on page 1-16 for more information.

Related Topics

- Understanding Security Profiles, page 1-12
- Identifying Authenticated, Encrypted, and Protected Phone Calls, page 1-13
- Establishing and Identifying Secure Conference Calls, page 1-14
- Device Configuration Menu, page 4-10
- Supporting 802.1X Authentication on Cisco Unified IP Phones, page 1-16
- Security Restrictions, page 1-17

Understanding Security Profiles

Cisco Unified IP Phones that support Cisco Unified Communications Manager 7.0 or later use a security profile, which defines whether the phone is nonsecure, authenticated, or encrypted. For information about configuring the security profile and applying the profile to the phone, refer to *Cisco Unified Communications Manager Security Guide*.

To view the security mode that is set for the phone, look at the Security Mode setting in the Security Configuration menu. For more information, see the "Security Configuration Menu" section on page 4-23.

Related Topics

- Identifying Authenticated, Encrypted, and Protected Phone Calls, page 1-13
- Device Configuration Menu, page 4-10
- Security Restrictions, page 1-17

Identifying Authenticated, Encrypted, and Protected Phone Calls

When security is implemented for a phone, you can identify authenticated or encrypted phone calls by icons on the screen that is on the phone.You can also determine if the connected phone is secure and protected if a security tone plays at the beginning of the call.

In an authenticated call, all devices participating in the establishment of the call are authenticated by Cisco Unified Communications Manager. When a call in progress is authenticated, the call progress icon to the right of the call duration timer in the phone screen changes to this icon:

In an encrypted call, all devices participating in the establishment of the call are authenticated by the Cisco Unified Communications Manager. In addition, call signaling and media streams are encrypted. An encrypted call offers a high level of security, providing integrity and privacy to the call. When a call in progress is being encrypted, the call progress icon to the right of the call duration timer in the phone screen changes to this icon:

Note If the call is routed through non-IP call legs, for example, PSTN, the call may be nonsecure even though it is encrypted within the IP network and has a lock icon associated with it.

In a protected call, a security tone plays at the beginning of a call to indicate that the other connected phone is also receiving and transmitting encrypted audio. If your call is connected to a non-protected phone, the security tone does not play.

Note Protected calling is supported for connections between two phones only. Some features, such as conference calling, shared lines, Extension Mobility, and Join Across Lines are not available when protected calling is configured. Protected calls are not authenticated.

Related Topic

- Understanding Security Features for Cisco Unified IP Phones, page 1-8
- Understanding Security Profiles, page 1-12
- Security Restrictions, page 1-17

Establishing and Identifying Secure Conference Calls

You can initiate a secure conference call and monitor the security level of participants. A secure conference call is established using this process:

1. A user initiates the conference from a secure phone (encrypted or authenticated security mode).
2. Cisco Unified Communications Manager assigns a secure conference bridge to the call.
3. As participants are added, Cisco Unified Communications Manager verifies the security mode of each phone (encrypted or authenticated) and maintains the secure level for the conference.
4. The phone displays the security level of the conference call. A secure conference displays (encrypted) or (authenticated) icon to the right of "Conference" on the phone screen. If icon displays, the conference is not secure.

Note There are interactions, restrictions, and limitations that affect the security level of the conference call depending on the security mode of the participant's phones and the availability of secure conference bridges. See Table 1-4 and Table 1-5 for information about these interactions.

Establishing and Identifying Protected Calls

A protected call is established when your phone, and the phone on the other end, is configured for protected calling. The other phone can be in the same Cisco Unified IP network, or on a network outside the IP network. Protected calls can only be made between two phones. Conference calls and other multiple-line calls are not supported.

A protected call is established using this process:

1. A user initiates the call from a protected phone (protected security mode).
2. The phone displays the icon (encrypted) on the phone screen. This icon indicates that the phone is configured for secure (encrypted) calls, but this does not mean that the other connected phone is also protected.
3. A security tone plays if the call is connected to another protected phone, indicating that both ends of the conversation are encrypted and protected. If the call is connected to a non-protected phone, then the secure tone is not played.

Note Protected calling is supported for conversations between two phones. Some features, such as conference calling, shared lines, Extension Mobility, and Join Across Lines are not available when protected calling is configured.

Call Security Interactions and Restrictions

Cisco Unified Communications Manager checks the phone security status when conferences are established and changes the security indication for the conference or blocks the completion of the call to maintain integrity and also security in the system. Table 1-4 provides information about changes to call security levels when using Barge.

Table 1-4 Call Security Interactions When Using Barge

Initiator's Phone Security Level	Feature Used	Call Security Level	Results of Action
Non-secure	Barge	Encrypted call	Call barged and identified as non-secure call
Secure (encrypted)	Barge	Authenticated call	Call barged and identified as authenticated call
Secure (authenticated)	Barge	Encrypted call	Call barged and identified as authenticated call
Non-secure	Barge	Authenticated call	Call barged and identified as non-secure call

Table 1-5 provides information about changes to conference security levels depending on the initiator's phone security level, the security levels of participants, and the availability of secure conference bridges.

Table 1-5 Security Restrictions with Conference Calls

Initiator's Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Non-secure	Conference	Encrypted or authenticated	Non-secure conference bridge Non-secure conference
Secure (encrypted or authenticated)	Conference	At least one member is non-secure	Secure conference bridge Non-secure conference
Secure (encrypted)	Conference	All participants are encrypted	Secure conference bridge Secure encrypted level conference
Secure (authenticated)	Conference	All participants are encrypted or authenticated	Secure conference bridge Secure authenticated level conference
Non-secure	Conference	Encrypted or authenticated	Only secure conference bridge is available and used Non-secure conference
Secure (encrypted or authenticated)	Conference	Encrypted or authenticated	Only non-secure conference bridge is available and used Non-secure conference
Secure (encrypted or authenticated)	Conference	Encrypted or secure	Conference remains secure. When one participant tries to hold the call with MOH, the MOH does not play.
Secure (encrypted)	Join	Encrypted or authenticated	Secure conference bridge Conference remains secure (encrypted or authenticated)

Table 1-5 Security Restrictions with Conference Calls (continued)

Initiator's Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Non-secure	cBarge	All participants are encrypted	Secure conference bridge Conference changes to non-secure
Non-secure	MeetMe	Minimum security level is encrypted	Initiator receives message "Does not meet Security Level", call rejected.
Secure (encrypted)	MeetMe	Minimum security level is authenticated	Secure conference bridge Conference accepts encrypted and authenticated calls
Secure (encrypted)	MeetMe	Minimum security level is non-secure	Only secure conference bridge available and used Conference accepts all calls

Supporting 802.1X Authentication on Cisco Unified IP Phones

These sections provide information about 802.1X support on the Cisco Unified IP Phones:

- Overview, page 1-16
- Required Network Components, page 1-16
- Best Practices—Requirements and Recommendations, page 1-17

Overview

Cisco Unified IP phones and Cisco Catalyst switches have traditionally used Cisco Discovery Protocol (CDP) to identify each other and to determine parameters such as VLAN allocation and inline power requirements. However, CDP is not used to identify any locally attached PCs. Therefore, Cisco Unified IP Phones provide an EAPOL pass-through mechanism, whereby a PC locally attached to the IP phone may pass through EAPOL messages to the 802.1X authenticator in the LAN switch. This capability prevents the IP phone from having to act as the authenticator, yet allows the LAN switch to authenticate a data end point prior to accessing the network.

In conjunction with the EAPOL pass-through mechanism, Cisco Unified IP Phones provide a proxy EAPOL-Logoff mechanism. If the locally attached PC is disconnected from the IP phone, the LAN switch would not see the physical link fail, because the link between the LAN switch and the IP phone is maintained. To avoid compromising network integrity, the IP phone sends an EAPOL-Logoff message to the switch on behalf of the downstream PC, which triggers the LAN switch to clear the authentication entry for the downstream PC.

The Cisco Unified IP phones contain an 802.1X supplicant in addition to the EAPOL pass-through mechanism. This supplicant allows network administrators to control the connectivity of IP phones to the LAN switch ports. The IP phone 802.1X supplicant implements the EAP-MD5 option for 802.1X authentication.

Required Network Components

Support for 802.1X authentication on Cisco Unified IP Phones requires several components, including:

- Cisco Unified IP Phone—The phone acts as the 802.1X supplicant, which initiates the request to access the network.
- Cisco Secure Access Control Server (ACS) (or other third-party authentication server)—The authentication server and the phone must both be configured with a shared secret that is used to authenticate the phone.
- Cisco Catalyst Switch (or other third-party switch)—The switch must support 802.1X to act as the *authenticator* and pass the messages between the phone and the authentication server. When the exchange is completed, the switch grants or denies the phone access to the network.

Best Practices—Requirements and Recommendations

- Enable 802.1X Authentication—If you want to use the 802.1X standard to authenticate Cisco Unified IP Phones, make sure that you have properly configured the other components before enabling it on the phone. See the "802.1X Authentication and Status" section on page 4-31 for more information.
- Configure PC Port—The 802.1X standard does not take into account the use of VLANs and thus recommends that only a single device be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multi-domain authentication. The switch configuration determines whether you can connect a PC to the phone PC port.
  - Enabled—If you are using a switch that supports multi-domain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco Unified IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, refer to the Cisco Catalyst switch configuration guides at:

    http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
  - Disabled—If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. See the "Security Configuration Menu" section on page 4-23 for more information. If you do not disable this port and subsequently attempt to attach a PC to it, the switch will deny network access to the phone and the PC.
- Configure Voice VLAN—Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
  - Enabled—If you are using a switch that supports multi-domain authentication, you can continue to use the voice VLAN.
  - Disabled—If the switch does not support multi-domain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN. See the "Security Configuration Menu" section on page 4-23 for more information.
- Enter MD5 Shared Secret—If you disable 802.1X authentication or perform a factory reset on the phone, the previously configured MD5 shared secret is deleted. See the "802.1X Authentication and Status" section on page 4-31 for more information.

Security Restrictions

A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. When barge fails in this case, a reorder tone (fast busy tone) plays on the phone on which the user initiated the barge.

If the initiator phone is configured for encryption, the barge initiator can barge into an authenticated or nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified Communications Manager classifies the call as nonsecure.

If the initiator phone is configured for encryption, the barge initiator can barge into an encrypted call, and the phone indicates that the call is encrypted.

A user can barge into an authenticated call, even if the phone that is used to barge is nonsecure. The authentication icon continues to appear on the authenticated devices in the call, even if the initiator phone does not support security.

Overview of Configuring and Installing Cisco Unified IP Phones

When deploying a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setting up and configuring a complete Cisco Unified IP telephony network, refer to the "System Configuration Overview" chapter in *Cisco Unified Communications Manager System Guide*.

After you have set up the IP telephony system and configured system-wide features in Cisco Unified Communications Manager, you can add IP phones to the system.

The following topics provide an overview of procedures for adding Cisco Unified IP Phones to your network:

- Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager, page 1-18
- Installing Cisco Unified IP Phones, page 1-21

Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager

To add phones to the Cisco Unified Communications Manager database, you can use:

- Auto-registration
- Cisco Unified Communications Manager Administration
- Bulk Administration Tool (BAT)
- BAT and the Tool for Auto-Registered Phones Support (TAPS)

For more information about these choices, see the "Adding Phones to the Cisco Unified Communications Manager Database" section on page 2-9.

For general information about configuring phones in Cisco Unified Communications Manager, refer to the "Cisco Unified IP Phone" chapter in *Cisco Unified Communications Manager System Guide* and to the "Cisco Unified IP Phone Configuration" chapter in *Cisco Unified Communications Manager Administration Guide*.

Checklist for Configuring the Cisco Unified IP Phone 7970 Series in Cisco Unified Communications Manager

Table 1-6 provides an overview and checklist of configuration tasks for the Cisco Unified IP Phone 7970 Series in Cisco Unified Communications Manager Administration. The list presents a suggested order to guide you through the phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table 1-6 Checklist for Configuring the Cisco Unified IP Phone 7970 Series

Task	Purpose	For More Information
1.	Gather the following information about the phone: • Phone Model • MAC address • Physical location of the phone • Name or user ID of phone user • Device pool • Partition, calling search space, and location information • Number of lines and associated directory numbers (DNs) to assign to the phone • Cisco Unified Communications Manager user to associate with the phone • Phone usage information that affects phone button template, softkey template, phone features, IP Phone services, or phone applications Provides list of configuration requirements for setting up phones. Identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates or softkey templates.	Refer to *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter. See the "Telephony Features Available for the Phone" section on page 5-1.
2.	Customize phone button templates (if required). Changes the number of line buttons, speed-dial buttons, Service URL buttons or adds a Privacy button to meet user needs.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter. See the"Modifying Phone Button Templates" section on page 5-17.
3.	Add and configure the phone by completing the required fields in the Phone Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, MAC address and device pool. Adds the device with its default settings to the Cisco Unified Communications Manager database.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter. For information about Product Specific Configuration fields, refer to "?" Button Help in the Phone Configuration window.

Table 1-6 Checklist for Configuring the Cisco Unified IP Phone 7970 Series (continued)

Task	Purpose	For More Information
4.	Add and configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, directory number and presence group. Adds primary and secondary directory numbers and features associated with directory numbers to the phone.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter, "Creating a Cisco Unity Voice Mailbox" section. See the "Telephony Features Available for the Phone" section on page 5-1.
5.	Customize softkey templates. Adds, deletes, or changes order of softkey features that display on the user's phone to meet feature usage needs.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Softkey Template Configuration" chapter. See the "Configuring Softkey Templates" section on page 5-19.
6.	Configure speed-dial buttons and assign speed-dial numbers (optional). Adds speed-dial buttons and numbers. **Note** Users can change speed-dial settings on their phones by using Cisco Unified CM User Options.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter, "Configuring Speed-Dial Buttons" section.
7.	Configure Cisco Unified IP Phone services and assign services (optional). Provides IP Phone services. **Note** Users can add or change services on their phones by using the Cisco Unified CM User Options web pages.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Services Configuration" chapter. See the "Setting Up Services" section on page 5-20.
8.	Assign services to phone buttons (optional). Provides single button access to an IP phone service or URL.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter, "Adding a Cisco Unified IP Phone Service to a Phone Button" section.
9.	Add user information by configuring required fields. Required fields are indicated by an asterisk (*); for example, User ID and last name. **Note** Assign a password (for User Options web pages) and PIN (for Extension Mobility and Personal Directory) Adds user information to the global directory for Cisco Unified Communications Manager.	Refer to *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" chapter. See the "Adding Users to Cisco Unified Communications Manager" section on page 5-20.

Table 1-6 Checklist for Configuring the Cisco Unified IP Phone 7970 Series (continued)

Task	Purpose	For More Information
10.	Associate a user to a user group. Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users.	Refer to the *Cisco Unified Communications Manager Administration Guide*: • "End User Configuration" chapter, "End User Configuration settings" section. • "User Group Configuration" chapter, "Adding Users to a User Group" section.
11.	Associate a user with a phone (optional). Provides users with control over their phone such as forwarding calls or adding speed-dial numbers or services. **Note** Some phones, such as those in conference rooms, do not have an associated user.	Refer to *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" chapter, "Associating Devices to a User" section.

Installing Cisco Unified IP Phones

After you have added the phones to the Cisco Unified Communications Manager database, you can complete the phone installation. You (or the phone users) can install the phone at the users's location. The Cisco Unified IP Phone Installation Guide, which is available on cisco.com, provides directions for connecting the phone handset, cables, and other accessories.

Note Before you install a phone, even if it is new, upgrade the phone to the current firmware image. For information about upgrading, refer to the Readme file for your phone, which is located at:

http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser

After the phone is connected to the network, the phone startup process begins and the phone registers with Cisco Unified Communications Manager. To finish installing the phone, configure the network settings on the phone depending on whether you enable or disable DHCP service.

If you used auto-registration, you need to update the specific configuration information for the phone such as associating the phone with a user, changing the button table, or directory number.

Checklist for Installing the Cisco Unified IP Phone 7970 Series

Table 1-7 provides an overview and checklist of installation tasks for the Cisco Unified IP Phone 7970 Series. The list presents a suggested order to guide you through the phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table 1-7 Checklist for Installing the Cisco Unified IP Phone 7970 Series

Task	Purpose	For More Information
1.	Choose the power source for the phone: • Power over Ethernet (PoE) • External power supply Determines how the phone receives power.	See the "Providing Power to the Phone" section on page 2-3.
2.	Assemble the phone, adjust phone placement, and connect the network cable. Locates and installs the phone in the network.	See the "Installing the Cisco Unified IP Phone" section on page 3-5. See the "Adjusting the Placement of the Cisco Unified IP Phone" section on page 3-8.
3.	Add a Cisco Unified IP Phone Expansion Module 7914 (optional). Extends functionality to a Cisco Unified IP Phone by adding 14 line appearances or speed dial numbers.	See the "Attaching the Cisco Unified IP Phone Expansion Module 7914" section on page 3-7.
4.	Monitor the phone startup process. Verifies that phone is configured properly.	See the "Verifying the Phone Startup Process" section on page 3-10.

Table 1-7 Checklist for Installing the Cisco Unified IP Phone 7970 Series (continued)

Task	Purpose	For More Information
5.	When you are configuring the network settings on the phone, you can set up an IP address for the phone by either using DHCP or manually entering an IP address. Using DHCP—To enable DHCP and allow the DHCP server to automatically assign an IP address to the Cisco Unified IP Phone and direct the phone to a TFTP server, choose **Settings > Network Configuration> IPv4 Configuration** and: • To enable DHCP, set DHCP Enabled to **Yes.** DHCP is enabled by default. • To use an alternate TFTP server, set Alternate TFTP Server to **Yes,** and enter the IP address for the TFTP Server. **Note** Consult with the network administrator if you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP. Without DHCP—You must configure the IP address, subnet mask, TFTP server, and default router locally on the phone, choose **Settings > Network Configuration> IPv4 Configuration**: To disable DHCP and manually set an IP address: **a.** To disable DHCP, set DHCP Enabled to **No**. **b.** Enter the static IP address for phone. **c.** Enter the subnet mask. **d.** Enter the default router IP addresses. **e.** Set Alternate TFTP Server to **Yes, and** enter the IP address for TFTP Server 1. You must also enter the domain name where the phone resides by Choosing **Settings > Network Configuration.**	See the "Configuring Startup Network Settings" section on page 3-11. See the "Network Configuration Menu" section on page 4-5.
6.	Set up security on the phone. Provides protection against data tampering threats and identity theft of phones.	See the "Configuring Security on the Cisco Unified IP Phone" section on page 3-12.
7.	Make calls with the Cisco Unified IP Phone. Verifies that the phone and features work correctly.	Refer to *Cisco Unified IP Phone 7970 Series Guide*.
8.	Provide information to end users about how to use their phones and how to configure their phone options. Ensures that users have adequate information to successfully use their Cisco Unified IP Phones.	See Appendix A, "Providing Information to Users Via a Website."

CHAPTER 2

Preparing to Install the Cisco Unified IP Phone on Your Network

Cisco Unified IP Phones enable you to communicate using voice over a data network. To provide this capability, the IP Phones depend upon and interact with several other key Cisco Unified IP Telephony and network components, including Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, media resources, Cisco prestandard PoE, and so on.

This chapter focuses on the interactions between the Cisco Unified IP Phone 7970 Series and Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, and switches. It also describes options for powering phones.

For related information about voice and IP communications, refer to this URL:

http://www.cisco.com/en/US/products/sw/voicesw/index.html

This chapter provides an overview of the interaction between the Cisco Unified IP Phone 7970 Series and other key components of the Voice over IP (VoIP) network. It includes these topics:

- Understanding Interactions with Other Cisco Unified IP Communications Products, page 2-2
- Providing Power to the Phone, page 2-3
- Understanding Phone Configuration Files, page 2-6
- Understanding the Phone Startup Process, page 2-7
- Adding Phones to the Cisco Unified Communications Manager Database, page 2-9
- Using Cisco Unified IP Phones with Different Protocols, page 2-12
- Determining the MAC Address of a Cisco Unified IP Phone, page 2-14

Understanding Interactions with Other Cisco Unified IP Communications Products

To function in the IP telephony network, the Cisco Unified IP Phone must be connected to a networking device, such as a Cisco Catalyst switch. You must also register the Cisco Unified IP Phone with a Cisco Unified Communications Manager system before sending and receiving calls.

This section includes these topics:

- Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager, page 2-2
- Understanding How the Cisco Unified IP Phone Interacts with the VLAN, page 2-3

Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager

Cisco Unified Communications Manager is an open and industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between phones, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the IP telephony system—the phones, the access gateways, and the resources necessary for features such as call conferencing and route planning. Cisco Unified Communications Manager also provides:

- Firmware for phones
- Authentication and encryption (if configured for the telephony system)
- Configuration file and CTL file, via TFTP service
- Phone registration
- Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

For information about configuring Cisco Unified Communications Manager to work with the IP devices described in this chapter, refer to *Cisco Unified Communications Manager Administration Guide*, *Cisco Unified Communications Manager System Guide*, and *Cisco Unified Communications Manager Security Guide.*

For an overview of security functionality for the Cisco Unified IP Phone, see the "Understanding Security Features for Cisco Unified IP Phones" section on page 1-8.

Note If the Cisco Unified IP Phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified Communications Manager Administration, go to the following URL and install the latest support patch for your version of Cisco Unified Communications Manager:

http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Related Topic

- Telephony Features Available for the Phone, page 5-1

Understanding How the Cisco Unified IP Phone Interacts with the VLAN

The Cisco Unified IP Phone 7970 Series have an internal Ethernet switch, enabling forwarding of packets to the phone, and to the access port and the network port on the back of the phone.

If a computer is connected to the access port, the computer and the phone share the same physical link to the switch and share the same port on the switch. This shared physical link has the following implications for the VLAN configuration on the network:

- The current VLANs might be configured on an IP subnet basis. However, additional IP address might not be available to assign the phone to the same subnet as other devices connect to the same port.
- Data traffic present on the data/native VLAN may reduce the quality of Voice-over-IP traffic.
- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN. The switch port that the phone is connected to would be configured to have separate VLANs for carrying:

- Voice traffic to and from the IP phone (auxiliary VLAN, on the Cisco Catalyst 6000 series, for example)
- Data traffic to and from the PC connected to the switch through the access port of the IP phone (native VLAN)

Isolating the phones on a separate, auxiliary VLAN improves the quality of the voice traffic and allows a large number of phones to be added to an existing network where there are not enough IP addresses for each phone.

For more information, refer to the documentation included with a Cisco switch. You can also access related documentation at this URL:

http://cisco.com/en/US/products/hw/switches/index.html

Related Topics

- Understanding the Phone Startup Process, page 2-7
- Network Configuration Menu, page 4-5

Providing Power to the Phone

Models in the Cisco Unified IP Phone 7970 Series can be powered with external power or with Power over Ethernet (PoE). External power is provided through a separate power supply. PoE is provided by a switch through the Ethernet cable attached to a phone.

Note When you install a phone that is powered with external power, connect the power supply to the phone and to a power outlet before you connect the Ethernet cable to the phone. When you remove a phone that is powered with external power, disconnect the Ethernet cable from the phone before you disconnect the power supply.

The following sections provide more information about powering a phone:

- Power Guidelines, page 2-4
- Phone Power Consumption and Display Brightness, page 2-5

- Power Outage, page 2-5
- Obtaining Additional Information about Power, page 2-6

Power Guidelines

Table 2-1 provides guidelines that apply to external power and to PoE power for phones the Cisco Unified IP Phone 7970 Series.

Table 2-1 Guidelines for Powering the Cisco Unified IP Phone 7970 Series

Power Type	Guidelines
External power— Provided through the CP-PWR-CUBE-3 external power supply	The Cisco Unified IP Phone Series uses the CP-PWR-CUBE-3 power supply.
External power— Provided through the Cisco Unified IP Phone Power Injector	The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector is connected between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the IP Phone.
PoE power—Provided by a switch through the Ethernet cable attached to the phone	• The inline power patch panel WS-PWR-PANEL is not compatible with the Cisco Unified IP Phone 7970 Series. • To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply. • Make sure that the CatOS or IOS version running on your switch supports your intended phone deployment. Refer to the documentation for your switch for operating system version information.

Phone Power Consumption and Display Brightness

The power consumed by a phone depends on its power configuration. See Table 2-1 for a power configuration overview. See Table 2-2 for the maximum power consumed by a phone for each configuration option and the correlating phone screen brightness level.

Note Power consumption values shown in the table include power losses in the cable that connects the phone to the switch.

Table 2-2 Power Consumption and Display Brightness for Power Configurations

Phone Model	Power Configuration	Max. Power Consumed from a Switch	Phone Screen Brightness
Cisco Unified IP Phone 7970G	Cisco prestandard PoE from a switch that supports a maximum of 7 W power per port, with bidirectional power negotiation enabled	6.3 W	Approx. 1/2
	Cisco prestandard PoE from a Cisco Switch that supports 7 W or 15.4 W power per port, without bidirectional power negotiation	6.3 W	Approx. 1/2
	IEEE 802.3af Class 3 power from a Cisco switch, without bidirectional power negotiation	6.3 W	Approx. 1/2
	IEEE 802.3af Class 3 power from a third-party switch	6.3 W	Approx. 1/2
	IEEE 802.3af Class 3 power from a Cisco switch, with bidirectional power negotiation enabled	10.25 W	Full[1]
	Cisco prestandard PoE from a Cisco Switch that supports 15.4 W power per port, with bidirectional power negotiation enabled	10.25 W	Full
	External power	—	Full
Cisco Unified IP Phone 7971G-GE	IEEE 802.3af Class 3 power from a Cisco switch (with or without bidirectional power negotiation enabled) or from a third-party switch	15.4 W	Near full
	External power	—	Full

1. Starts at approximately 1/2 brightness, changes to full brightness when the phone negotiates additional power.

Note When a phone is powered with a method that does not support full brightness for the phone screen, the phone Brightness control (**Settings > User Preferences > Brightness**) does not allow you to set the brightness to the maximum value.

Power Outage

Your accessibility to emergency service through the phone is dependent on the phone being powered. If there is an interruption in the power supply, Service and Emergency Calling Service dialing will not function until power is restored. In the case of a power failure or disruption, you may need to reset or reconfigure equipment before using the Service or Emergency Calling Service dialing.

Obtaining Additional Information about Power

For related information about power, refer to the documents shown in Table 2-3. These documents provide information about these topics:

- Cisco switches that work with the Cisco Unified IP Phone 7970 Series
- The Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions regarding power

Table 2-3 Related Documentation for Power

Document Topics	URL
Cisco Unified IP Phone Power Injector	http://www.cisco.com/en/US/products/hw/phones/ps379/prod_installation_guides_list.html
PoE Solutions	http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns412/networking_solutions_package.html
Cisco Catalyst Switches	http://cisco.com/en/US/products/hw/switches/index.html
Integrated Service Routers	http://www.cisco.com/en/US/products/hw/routers/index.html
Cisco IOS Software	http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html

Understanding Phone Configuration Files

Configuration files for a phone are stored on the TFTP server and define parameters for connecting to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified Communications Manager that requires the phone to be reset, a change is automatically made to the phone's configuration file.

Configuration files also contain information about which image load the phone should be running. If this image load differs from the one that is currently loaded on a phone, the phone contacts the TFTP server to request the required load files. (These files are digitally signed to ensure the authenticity of the file source.)

In addition, if the device security mode in the configuration file is set to Authenticated and the CTL file on the phone has a valid certificate for Cisco Unified Communications Manager, the phone establishes a TLS connection to Cisco Unified Communications Manager. Otherwise, the phone establishes a TCP connection. For SIP phones, a TLS connection requires that the transport protocol in the phone configuration file be set to TLS, which corresponds to the transport type in the SIP Security Profile in Cisco Unified Communications Manager.

Note If the device security mode in the configuration file is set to Authenticated or Encrypted, but the phone has not received a CTL file, the phone continuously tries to obtain a CTL file so it can register securely.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, refer to the "Configuring Encrypted Phone Configuration Files" chapter in *Cisco Unified Communications Manager Security Guide*.

A phone accesses a default configuration file named XmlDefault.cnf.xml from the TFTP server when these conditions exist:

- You have enabled auto-registration in Cisco Unified Communications Manager
- The phone has not been added to the Cisco Unified Communications Manager Database
- The phone is registering for the first time

If auto registration is not enabled and the phone has not been added to the Cisco Unified Communications Manager database, the phone registration request will be rejected. In this case, the phone resets and attempts to register repeatedly.

If the phone has registered before, the phone accesses the configuration file named SEP*mac_address*.cnf.xml, where *mac_address* is the MAC address of the phone.

For SIP phones, the TFTP server generates these SIP configuration files:

- SIP IP Phone:
  - For unsigned and unencrypted files—SEP<*mac*>.cnf.xml
  - For signed files—SEP<*mac*>.cnf.xml.sgn
  - For signed and encrypted files—SEP<*mac*>.cnf.xml.enc.sgn
- Dial Plan—<*dialplan*>.xml
- Softkey Template—<*softkey_template*>.xml

The filenames are derived from the MAC Address and Description fields in the Phone Configuration window of Cisco Unified Communications Manager Administration. The MAC address uniquely identifies the phone. For more information refer to *Cisco Unified Communications Manager Administration Guide*.

For more information about how the phone interacts with the TFTP server, refer to *Cisco Unified Communications Manager System Guide*, "Cisco TFTP" chapter.

Understanding the Phone Startup Process

When connecting to the VoIP network, the Cisco Unified IP Phone goes through a standard startup process, as described in Table 2-4. Depending on your specific network configuration, not all of these process steps may occur on your Cisco Unified IP Phone.

Table 2-4 Cisco Unified IP Phone Startup Process

Task	Purpose	Related Topics
1.	Obtaining Power from the Switch. If a phone is not using external power, the switch provides in-line power through the Ethernet cable that is attached to the phone.	See the "Providing Power to the Phone" section on page 2-3. See the "Resolving Startup Problems" section on page 9-1.
2.	Loading the StoredPhone Image. The Cisco Unified IP Phone has non-volatile flash memory in which it stores firmware images and user-defined preferences. At startup, the phone runs a bootstrap loader that loads a phone image stored in flash memory. Using this image, the phone initializes its software and hardware.	See the "Resolving Startup Problems" section on page 9-1.

Table 2-4 Cisco Unified IP Phone Startup Process (continued)

Task	Purpose	Related Topics
3.	Configuring VLAN. If the Cisco Unified IP Phone is connected to a Cisco switch, the switch next informs the phone of the voice VLAN defined on the switch port. The phone needs to know its VLAN membership before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address.	See the "Network Configuration Menu" section on page 4-5. See the "Resolving Startup Problems" section on page 9-1.
4.	Obtaining an IP Address. If the Cisco Unified IP Phone is using DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each phone locally.	See the "Network Configuration Menu" section on page 4-5. See the "Resolving Startup Problems" section on page 9-1.
5.	Accessing a TFTP Server. on to assigning an IP address, the DHCP server directs the Cisco Unified IP Phone to a TFTP Server. If the phone has a statically defined IP address, you must configure the TFTP server locally on the phone; the phone then contacts the TFTP server directly. **Note** You can also assign an alternative TFTP server to use instead of the one assigned by DHCP.	See the "Network Configuration Menu" section on page 4-5. See the "Resolving Startup Problems" section on page 9-1.
6.	Requesting the CTL file. The TFTP server stores the certificate trust list (CTL) file. This file contains a list of Cisco Unified Communications Managers and TFTP servers that the phone is authorized to connect to. It also contains the certificates necessary for establishing a secure connection between the phone and Cisco Unified Communications Manager.	Refer to *Cisco Unified Communications Manager Security Guide,* "Configuring the Cisco CTL Client" chapter.

Table 2-4 Cisco Unified IP Phone Startup Process (continued)

Task	Purpose	Related Topics
7.	Requesting the Configuration File. The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the phone.	See the "Understanding Phone Configuration Files" section on page 2-6. See the "Resolving Startup Problems" section on page 9-1.
8.	Contacting Cisco Unified Communications Manager. The configuration file defines how the Cisco Unified IP Phone communicates with Cisco Unified Communications Manager and provides a phone with its load ID. After obtaining the file from the TFTP server, the phone attempts to make a connection to the highest priority Cisco Unified Communications Manager on the list. If security is implemented, the phone makes a TLS connection. Otherwise, it makes a non-secure TCP connection. If the phone was manually added to the database, Cisco Unified Communications Manager identifies the phone. If the phone was not manually added to the database and auto-registration is enabled in Cisco Unified Communications Manager, the phone attempts to auto-register itself in the Cisco Unified Communications Manager database. **Note** Auto-registration is disabled when security is enabled on Cisco Unified Communications Manager. In this case, the phone must be manually added to the Cisco Unified Communications Manager database.	See the "Resolving Startup Problems" section on page 9-1.

Adding Phones to the Cisco Unified Communications Manager Database

Before installing the Cisco Unified IP phone, you must choose a method for adding phones to the Cisco Unified Communications Manager database. These sections describe the methods:

- Adding Phones with Auto-Registration, page 2-10
- Adding Phones with Auto-Registration and TAPS, page 2-11
- Adding Phones with Cisco Unified Communications Manager Administration, page 2-12
- Adding Phones with BAT, page 2-12

Table 2-5 provides an overview of these methods for adding phones to the Cisco Unified Communications Manager database.

Table 2-5 Methods for Adding Phones to the Cisco Unified Communications Manager Database

Method	Requires MAC Address?	Notes
Auto-registration	No	• Results in automatic assignment of directory numbers. • Not available when security or encryption is enabled.
Auto-registration with TAPS	No	Requires auto-registration and the Bulk Administration Tool (BAT); updates the Cisco Unified Communications Manager database with the MAC address and DNs for the device when user calls TAPS from the phone.
Using the Cisco Unified Communications Manager Administration	Yes	Requires phones to be added individually
Using BAT	Yes	Can add groups of same model of phone. Can schedule when phones are added to the Cisco Unified Communications Manager database.

Adding Phones with Auto-Registration

By enabling auto-registration before you begin installing phones, you can:

- Add phones without first gathering MAC addresses from the phones.
- Automatically add a Cisco Unified IP Phone to the Cisco Unified Communications Manager database when you physically connect the phone to your IP telephony network. During auto-registration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone.
- Quickly enter phones into the Cisco Unified Communications Manager database and modify any settings, such as the directory numbers, from Cisco Unified Communications Manager.
- Move auto-registered phones to new locations and assign them to different device pools without affecting their directory numbers.

Note Cisco recommends you use auto-registration to add less than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). See the "Adding Phones with BAT" section on page 2-12.

Auto-registration is disabled by default. In some cases, you might not want to use auto-registration; for example, if you want to assign a specific directory number to the phone or if you plan to implement authentication or encryption, as described in *Cisco Unified Communications Manager Security Guide*. For information about enabling auto-registration, refer to "Enabling Auto-Registration" in the *Cisco Unified Communications Manager Administration Guide.*

Note When you configure the cluster for mixed mode through the Cisco CTL client, auto-registration is automatically disabled. When you configure the cluster for non-secure mode through the Cisco CTL client, auto-registration is automatically enabled.

Related Topics

- Adding Phones with Auto-Registration and TAPS, page 2-11
- Adding Phones with Cisco Unified Communications Manager Administration, page 2-12
- Adding Phones with BAT, page 2-12

Adding Phones with Auto-Registration and TAPS

You can add phones with auto-registration and TAPS, the Tool for Auto-Registered Phones Support, without first gathering MAC addresses from phones.

TAPS works with the Bulk Administration Tool (BAT) to update a batch of phones that were already added to the Cisco Unified Communications Manager database with dummy MAC addresses. Use TAPS to update MAC addresses and download pre-defined configurations for phones.

Note Cisco recommends you use auto-registration and TAPS to add less than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). See the "Adding Phones with BAT" section on page 2-12.

To implement TAPS, you or the end-user dial a TAPS directory number and follow voice prompts. When the process is complete, the phone will have downloaded its directory number and other settings, and the phone will be updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Auto-registration must be enabled in Cisco Unified Communications Manager Administration (**System > Cisco Unified CM**) for TAPS to function.

Note When you configure the cluster for mixed mode through the Cisco CTL client, auto-registration is automatically disabled. When you configure the cluster for non-secure mode through the Cisco CTL client, auto-registration is automatically enabled.

Refer to *Cisco Unified Communications Manager Bulk Administration Guide* for detailed instructions about BAT and about TAPS.

Related Topics

- Adding Phones with Auto-Registration, page 2-10
- Adding Phones with Cisco Unified Communications Manager Administration, page 2-12
- Adding Phones with BAT, page 2-12

Adding Phones with Cisco Unified Communications Manager Administration

You can add phones individually to the Cisco Unified Communications Manager database using Cisco Unified Communications Manager Administration. To do so, you first need to obtain the MAC address for each phone.

For information about determining a MAC address, see the "Determining the MAC Address of a Cisco Unified IP Phone" section on page 2-14.

After you have collected MAC addresses, in Cisco Unified Communications Manager Administration, choose **Device > Phone** and click **Add New** to begin.

For complete instructions and conceptual information about Cisco Unified Communications Manager, refer to *Cisco Unified Communications Manager Administration Guide* and to *Cisco Unified Communications Manager System Guide*.

Related Topics

- Adding Phones with Auto-Registration, page 2-10
- Adding Phones with Auto-Registration and TAPS, page 2-11
- Adding Phones with BAT, page 2-12

Adding Phones with BAT

Cisco Unified Communications Manager Bulk Administration Tool (BAT), a standard Cisco Unified Communications Manager application, enables you to perform batch operations, which includes registration, on multiple phones.

To add phones using BAT only (not in conjunction with TAPS), you first need to obtain the appropriate MAC address for each phone.

For information about determining a MAC address, see the "Determining the MAC Address of a Cisco Unified IP Phone" section on page 2-14.

For detailed instructions about using BAT, refer to *Cisco Unified Communications Manager Bulk Administration Guide*.

Related Topics

- Adding Phones with Auto-Registration, page 2-10
- Adding Phones with Auto-Registration and TAPS, page 2-11
- Adding Phones with Cisco Unified Communications Manager Administration, page 2-12

Using Cisco Unified IP Phones with Different Protocols

The Cisco Unified IP Phone can operate with SCCP (Skinny Client Control Protocol) or SIP (Session Initiation Protocol). You can convert a phone that is using one protocol for use with the other protocol.

This section includes these topics:

- Converting a New Phone from SCCP to SIP, page 2-13
- Converting an In-Use Phone from SCCP to SIP, page 2-13

- Converting an In-Use Phone from SIP to SCCP, page 2-13
- Deploying a Phone in an SCCP and SIP Environment, page 2-14

Converting a New Phone from SCCP to SIP

A new, unused phone is set for SCCP by default. To convert this phone to SIP, perform these steps:

Procedure

Step 1 Take one of these actions:

- To auto-register the phone, set the Auto Registration Phone Protocol parameter in Cisco Unified Communications Manager Administration to SIP.
- To provision the phone using the Bulk Administration Tool (BAT), choose the appropriate phone model and choose SIP from the BAT.
- To provision the phone manually, make the appropriate changes for SIP on the Phone configuration window in Cisco Unified Communications Manager Administration.

Refer to *Cisco Unified Communications Manager Administration Guide* for detailed information about Cisco Unified Communications Manager configuration. Refer to *Cisco Unified Communications Manager Bulk Administration Guide* for detailed information about using the BAT.

Step 2 If you are not using DHCP in your network, configure the network parameters for the phone.

See the “Configuring Startup Network Settings” section on page 3-14.

Step 3 Save the configuration updates, reset the phone, and have the user power cycle the phone.

Converting an In-Use Phone from SCCP to SIP

You can use the Bulk Administration Tool (BAT) to convert a phone that is in use in your network from SCCP to SIP. To access BAT from Cisco Unified Communications Manager Administration, choose **Bulk Administration > Phones > Migrate Phones > SCCP to SIP**. For detailed information, refer to *Cisco Unified Communications Manager Bulk Administration Guide*.

Converting an In-Use Phone from SIP to SCCP

To convert a phone that is in use in your network from SIP to SCCP, perform these steps. For more information, *Cisco Unified Communications Manager Administration Guide*.

Tip Before deleting a SIP phone (that you want to convert to a SCCP phone) from the Cisco Unified Communications Manager database, copy all of the phone configuration information, so when you add the phone back to the database, you will have the configuration information readily available.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, delete the existing SIP phone from the Cisco Unified Communications Manager database.

Step 2 In Cisco Unified Communications Manager Administration, create the phone as an SCCP phone.

Step 3 Power cycle the phone.

Deploying a Phone in an SCCP and SIP Environment

To deploy Cisco Unified IP Phones in an environment that includes SCCP and SIP and in which the Cisco Unified Communications Manager Auto-Registration parameter is SCCP, perform these general steps:

1. Set the Cisco Unified Communications Manager auto_registration_protocol parameter to SCCP.

   From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
2. Install the phones.
3. Change the Auto Registration Protocol enterprise parameter to SIP.
4. Auto-register the SIP phones.

Determining the MAC Address of a Cisco Unified IP Phone

Several of the procedures that are described in this manual require you to determine the MAC address of a Cisco Unified IP Phone. You can determine the MAC address for a phone in any of these ways:

- From the phone, choose **Settings > Network Configuration** and look at the MAC Address field.
- Look at the MAC label on the back of the phone.
- Display the web page for the phone and click the **Device Information** hyperlink.

  For information about accessing the web page, see the "Accessing the Web Page for a Phone" section on page 8-1.

CHAPTER 3

Setting Up the Cisco Unified IP Phone

This chapter includes the following topics, which help you install the Cisco Unified IP Phone 7970 Series on an IP telephony network:

- Before You Begin, page 3-1
- Understanding the Cisco Unified IP Phone 7970 Series Components, page 3-2
- Installing the Cisco Unified IP Phone, page 3-5
- Attaching the Cisco Unified IP Phone Expansion Module 7914, page 3-7
- Adjusting the Placement of the Cisco Unified IP Phone, page 3-8
- Verifying the Phone Startup Process, page 3-10
- Configuring Startup Network Settings, page 3-11
- Configuring Security on the Cisco Unified IP Phone, page 3-12

Note Before you install a Cisco Unified IP phone, you must decide how to configure the phone in your network. Then you can install the phone and verify its functionality. For more information, see Chapter 2, "Preparing to Install the Cisco Unified IP Phone on Your Network."

Before You Begin

Before installing the Cisco Unified IP Phone, review the requirements in these sections:

- Network Requirements, page 3-1
- Cisco Unified Communications Manager Configuration, page 3-2

Network Requirements

For the Cisco Unified IP Phone 7970 Series to successfully operate as a Cisco Unified IP Phone endpoint in your network, your network must meet these requirements:

- Working Voice over IP (VoIP) network:
  - VoIP configured on your Cisco routers and gateways
  - Cisco Unified Communications Manager Release 7.0 or higher installed in your network and configured to handle call processing

- IP network that supports DHCP or manual assignment of IP address, gateway, and subnet mask

Note The Cisco Unified IP Phone displays the date and time from Cisco Unified Communications Manager. If the Cisco Unified Communications Manager server is located in a different time zone than the phones, the phones will not display the correct local time.

Cisco Unified Communications Manager Configuration

The Cisco Unified IP Phone requires Cisco Unified Communications Manager to handle call processing. Refer to *Cisco Unified Communications Manager Administration Guide* or to context-sensitive help in the Cisco Unified Communications Manager application to ensure that Cisco Unified Communications Manager is set up properly to manage the phone and to properly route and process calls.

If you plan to use auto-registration, verify that it is enabled and properly configured in Cisco Unified Communications Manager before connecting any Cisco Unified IP Phone to the network. For information about enabling and configuring auto-registration, refer to *Cisco Unified Communications Manager Administration Guide*. Also, see the "Adding Phones to the Cisco Unified Communications Manager Database" section on page 2-9.

You must use Cisco Unified Communications Manager to configure and assign telephony features to the Cisco Unified IP Phones. See the "Telephony Features Available for the Phone" section on page 5-1 for details.

In Cisco Unified Communications Manager, you can add users to the database and associate them with specific phones. In this way, users gain access to web pages that allow them to configure items such as call forwarding, speed dialing, and voice messaging system options. See the "Adding Users to Cisco Unified Communications Manager" section on page 5-20 for details.

Understanding the Cisco Unified IP Phone 7970 Series Components

The Cisco Unified IP Phone 7970 Series includes these components on the phone or as accessories for the phone:

- Network and Access Ports, page 3-2
- Handset, page 3-3
- Speakerphone, page 3-3
- Headset, page 3-3

Network and Access Ports

The back of the Cisco Unified IP Phone includes these ports:

- Network port—Labeled 10/100 SW on the Cisco Unified IP Phone 7970G and 10/100/1000 SW on the Cisco Unified IP Phone 7971G-GE
- Access port—Labeled 10/100 PC on the Cisco Unified IP Phone 7970G and 10/100/1000 PC on the Cisco Unified IP Phone 7971G-GE

Each port supports 10/100 or 10/100/1000 Mbps half- or full-duplex connections to external devices. You can use either Category 3 or 5 cabling for 10-Mbps connections, but you must use Category 5 for 100 and 1000 Mbps connections.

Use the SW network port to connect the phone to the network. You must use a straight-through cable on this port. The phone can also obtain inline power from a switch over this connection. See the "Providing Power to the Phone" section on page 2-3 for details.

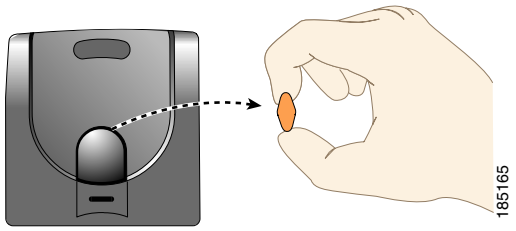
Use the PC access port to connect a network device, such as a computer, to the phone. You must use a straight-through cable on this port.

Handset

The handset is designed especially for use with a Cisco Unified IP Phone. It includes a light strip that indicates incoming calls and voice messages waiting.

To connect a handset to the Cisco Unified IP Phone, remove the hookswitch clip from the cradle area, as shown in Figure 3-1. Then plug the cable into the handset and into the Handset port on the back of the phone.

Figure 3-1 Removing the Hookswitch Clip



Speakerphone

By default, the speakerphone is enabled on Cisco Unified IP Phone 7970 Series.

You can disable the speakerphone by using Cisco Unified Communications Manager Administration. To do so, choose **Device > Phone** and locate the phone you want to modify. In the Phone Configuration for the phone, check the **Disable Speakerphone** check box.

Headset

Although Cisco Systems performs internal testing of third-party headsets for use with the Cisco Unified IP Phones, Cisco does not certify or support products from headset or handset vendors.

Cisco recommends the use of good quality external devices, for example, headsets that are screened against unwanted radio frequency (RF) and audio frequency (AF) signals. Depending on the quality of headsets and their proximity to other devices, such as mobile phones and two-way radios, some audio noise or echo may still occur. An audible hum or buzz may be heard by either the remote party of by both the remote party and the Cisco Unified IP Phone user. Humming or buzzing sounds can be caused by a range of outside sources; for example, electric lights, electric motors, or large PC monitors. See Using External Devices, page 3-4, for more information.

Note In some cases, hum may be reduced or eliminated by using a local power cube or power injector.

These environmental and hardware inconsistencies in the locations where Cisco Unified IP Phones are deployed means that there is not a single headset solution that is optimal for all environments.

Cisco recommends that customers test headsets in their intended environment to determine performance before making a purchasing decision and deploying en mass.

Note The Cisco Unified IP Phone 7970G/7971G-GE supports wideband headsets.

Audio Quality Subjective to the User

Beyond the physical, mechanical and technical performance, the audio portion of a headset must sound good to the user and the party on the far end. Sound quality is subjective and Cisco cannot guarantee the performance of any headsets or handsets. However, a variety headsets from leading headset manufacturers have been reported to perform well with Cisco Unified IP Phones. See manufacturer's sites for details.

Connecting a Headset

To connect a headset to the Cisco Unified IP Phone, plug it into the Headset port on the back of the phone. Press the **Headset** button on the phone to place and answer calls by using the headset.

You can use the headset with all of the features on the Cisco Unified IP Phone, including the Volume and Mute buttons. Use these buttons to adjust the ear piece volume and to mute the speech path from the headset microphone.

Disabling a Headset

You can disable the headset by using Cisco Unified Communications Manager Administration. If you do so, you also will disable the speakerphone.

To disable the headset from Cisco Unified Communications Manager Administration, choose **Device > Phone** and locate the phone that you want to modify. In the Phone Configuration for the phone, check the **Disable Speakerphone and Headset** check box.

Using External Devices

The following information applies when you use external devices with the Cisco Unified IP Phone:

Cisco recommends the use of good quality external devices that are shielded (screened) against unwanted radio frequency (RF) and audio frequency (AF) signals.

Depending on the quality of these devices and their proximity to other devices such as mobile phones or two-way radios, some audio noise may still occur. In these cases, Cisco recommends that you take one or more of the following actions:

- Move the external device away from the source of the RF or AF signals.
- Route the external device cables away from the source of the RF or AF signals.
- Use shielded cables for the external device, or use cables with a better shield and connector.

- Shorten the length of the external device cable.
- Apply ferrites or other such devices on the cables for the external device.

Cisco cannot guarantee the performance of the system because Cisco has no control over the quality of external devices, cables, and connectors. The system will perform adequately when suitable devices are attached using good quality cables and connectors.

Caution In European Union countries, use only external headsets that are fully compliant with the EMC Directive [89/336/EC].

Installing the Cisco Unified IP Phone

You must connect the Cisco Unified IP Phone to the network and to a power source before using it. Table 3-1 describes the tasks. See Figure 3-2 for a graphical representation of the connections.

Note Before you install a phone, even if it is new, upgrade the phone to the current firmware image.

Before using external devices, read the "Using External Devices" section on page 3-4 for safety and performance information.

Before You Begin

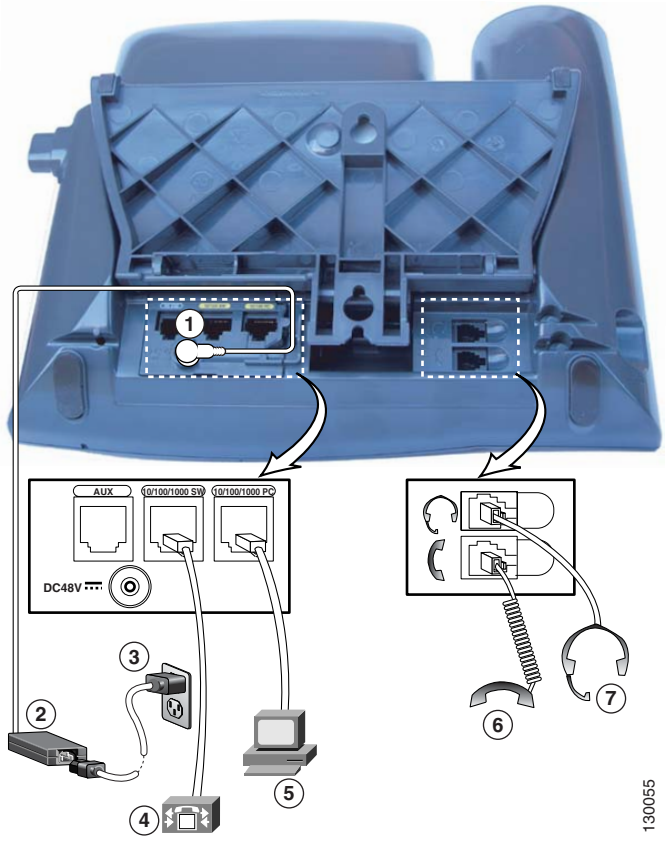
Remove the hookswitch clip (see the "Handset" section on page 3-3) from the cradle area.

To install a Cisco Unified IP Phone, perform the following steps:

Table 3-1 Installing the Cisco Unified IP Phone 7970G-7971G-GE

Task	Purpose	Related Topics
1.	Connect the handset to the Handset port.	—
2.	Connect a headset to the Headset port. Optional. You can add a headset later if you do not connect one now.	See the "Headset" section on page 3-3 for supported headsets.
3.	Connect the power supply to the Cisco DC Adapter portOptional.	See the "Providing Power to the Phone" section on page 2-3.
4.	Connect a Category 3 or 5 straight-through Ethernet cable from the switch to the 10/100 SW port (Cisco Unified IP Phone 7970) or the 10/100/1000 SW port (Cisco Unified IP Phone 7971G-GE). Each Cisco Unified IP Phone ships with one Ethernet cable in the box.	See the "Network and Access Ports" section on page 3-2 for guidelines.
5.	Connect a Category 3 or 5 straight-through Ethernet cable from another network device, such as a desktop computer, to the 10/100 PC port (Cisco Unified IP Phone 7970) or the 10/100/1000 PC port (Cisco Unified IP Phone 7971G-GE). Optional. You can connect another network device later if you do not connect one now.	See the "Network and Access Ports" section on page 3-2 for guidelines.

Figure 3-2 Cisco Unified IP Phone 7970 Series Rear Cable Connections



1	DC adapter port (DC48V)	**5**	Access port (1000 appears on the Cisco Unified IP Phone 7971G-GE only)
2	Power supply with DC Connector	**6**	Handset port
3	Power cable with AC wall plug	**7**	Headset port
4	Network port (1000 appears on the Cisco Unified IP Phone 7971G-GE only)		

Related Topics

- Before You Begin, page 3-1
- Attaching the Cisco Unified IP Phone Expansion Module 7914
- Adjusting the Placement of the Cisco Unified IP Phone, page 3-8
- Configuring Startup Network Settings, page 3-11

Attaching the Cisco Unified IP Phone Expansion Module 7914

The Cisco Unified IP Phone Expansion Module 7914 can be attached to Cisco Unified IP Phone 7970 Series to extend the number of line appearances or speed dial buttons. You can customize the button templates for the Cisco Unified IP Phone Expansion Module 7914 to determine the number of line appearances and speed dial buttons. See the "Modifying Phone Button Templates" section on page 5-17 for details.

You can attach a Cisco Unified IP Phone Expansion Module 7914 to a phone:

- When you initially add the phone to Cisco Unified Communications Manager by selecting **7914 14-Button Line Expansion Module** in the Module 1 or Module 2 fields and selecting the appropriate expansion module firmware. See Step 6 in the following procedure.
- After the phone is configured in Cisco Unified Communications Manager.

To configure the Cisco Unified IP Phone Expansion Module 7914 on a Cisco Unified IP Phone, follow these steps:

Procedure

Step 1 Log in to Cisco Unified Communications Manager Administration.

Cisco Unified Communications Manager Administration displays.

Step 2 From the menu, choose **Device > Phone**.

The Find and List Phone window displays. You can search for one or more phones that you want to configure for the Cisco Unified IP Phone Expansion Module 7914.

Step 3 Select and enter your search criteria and click **Find**.

The Find and List Phone window redisplays and shows a list of the phones that match your search criteria.

Step 4 Click the IP Phone that you want to configure for the Cisco Unified IP Phone Expansion Module 7914.

The Phone configuration window displays.

Step 5 Scroll to the Phone Button and Expansion Module Template Information section.

Step 6 Add support for expansion modules:

- To add one expansion module, in the Module 1 field, choose **7914 14-Button Line Expansion Module**.
- To add a second expansion module, in the Module 2 field, choose **7914 14-Button Line Expansion Module.**

In the Firmware Load Information section, there are two fields for specifying the firmware load for Modules 1 and 2. You can leave these fields blank to use the default firmware load.

Step 7 Scroll to the top of the page and click **Update**.

A message displays asking you to reset the phone for the changes to take effect. Click **OK**.

Step 8 Click **Reset Phone** for the changes to take effect.

Note Refer users to their User Options web pages so they can configure buttons and program buttons to access phone services on the Cisco Unified IP Phone Expansion Module 7914. See the "How Users Subscribe to Services and Configure Phone Features" section on page A-3 for more details.

Related Topics

- Before You Begin, page 3-1
- Adjusting the Placement of the Cisco Unified IP Phone, page 3-8
- Configuring Startup Network Settings, page 3-11

Adjusting the Placement of the Cisco Unified IP Phone

The Cisco Unified IP Phone includes an adjustable footstand. When placing the phone on a desktop surface, you can adjust the tilt height to several different angles in 7.5 degree increments from flat to 60 degrees. You can also mount the phone to the wall by using the footstand or by using the optional locking wall mount kit.

Adjusting Cisco Unified IP Phone Footstand and Phone Height

You can adjust the footstand adjustment plate on the Cisco Unified IP Phone to the height that provides optimum viewing of the phone screen. See Figure 3-4 for more information.

Procedure

Step 1 Push in the footstand adjustment button.

Step 2 Adjust the footstand to the desired height.

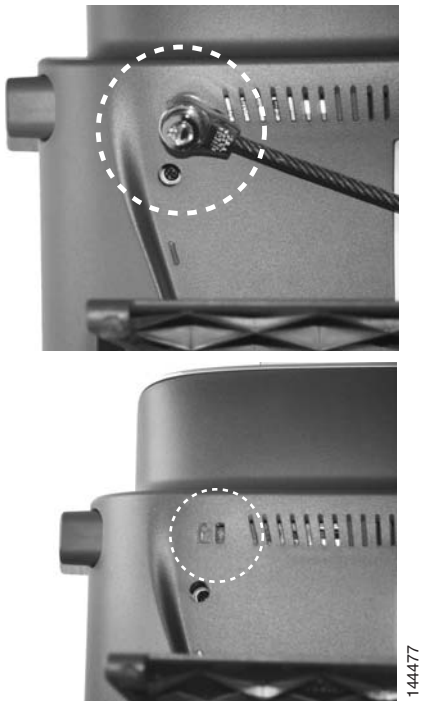
Securing the Phone with a Cable Lock

You can secure the Cisco Unified IP Phone 7970G and 7971G-GE to a desktop by using a laptop cable lock. The lock connects to the security slot on the back of the phone, and the cable can be secured to a desktop.

The security slot can accommodate a lock up to 20 mm. Compatible laptop cable locks include the Kensington laptop cable lock and laptop cable locks from other manufacturers that can fit into the security slot on the back of the phone.

See Figure 3-3.

Figure 3-3 Connecting a Cable Lock to the Cisco Unified IP Phone 7970 Series



Mounting the Phone to the Wall

You can mount the Cisco Unified IP Phone on the wall by using the footstand as a mounting bracket or you can use special brackets available in a Cisco Unified IP Phone wall mount kit. (Wall mount kits must be ordered separately from the phones.) If you attach the phone to a wall by using the standard footstand and not the wall mount kit, you need to supply the following tools and parts:

- Screwdriver
- Screws to secure the Cisco Unified IP phone to the wall

See Figure 3-4 for a graphical representation of the phone parts.

Before You Begin

To ensure that the handset attaches securely to a wall-mounted phone, remove the handset wall hook from the handset rest, rotate the hook 180 degrees, and reinsert the hook. Turning the hook exposes a lip on which the handset catches when the phone is vertical. For an illustrated procedure, refer to *Installing the Wall Mount Kit for the Cisco Unified IP Phone at*:

http://www.cisco.com/en/US/products/hw/phones/ps379/prod_installation_guides_list.html

To mount the phone on the wall by using the standard footstand, follow these steps:

Caution Use care not to damage wires or pipes located inside the wall when securing screws to wall studs.

Procedure

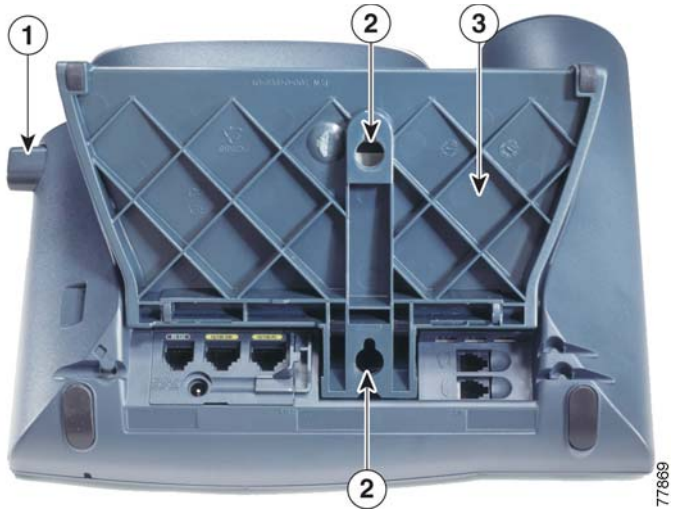
Step 1 Push in the footstand adjustment button.

Step 2 Adjust the footstand so it is flat against the back of the phone.

Step 3 Insert two screws into a wall stud, matching them to the two screw holes on the back of the footstand. The keyholes fit standard phone jack mounts.

Step 4 Hang the phone on the wall.

Figure 3-4 Parts Used in Wall Mounting the Cisco Unified IP Phone



1	Footstand adjustment button—Raises and lowers adjustment plate
2	Wall mounting screw holes
3	Adjustment plate—Raises and lowers phone vertically

Verifying the Phone Startup Process

After the Cisco Unified IP Phone has power connected to it, the phone begins its startup process by cycling through these steps.

1. These buttons flash on and off in sequence:
   - Headset. (Only if the handset is off-hook when the phone powers up. In this case, hang up the handset within 3 seconds or the phone launches its secondary load instead of its primary load.)
   - Mute.
   - Speaker.
2. Some or all of the line keys flash orange.

Caution If the line keys flash red in sequence after flashing yellow, do not power down the phone until the sequence of red flashes completes. This sequence can take several minutes to complete.

3. Some or all of the line keys flash green.

   Normally, this sequence takes just a few seconds. However, if the phone flash memory is erased or the phone load is corrupted, the sequence of green flashes will continue while the phone begins a software update procedure. If the phone performs this procedure, the following buttons light to indicate progress:

   - Headset—Phone is waiting for the network and completing CDP and DHCP configuration. (A DHCP server must be available in your network.)
   - Mute—Phone is downloading images from the TFTP server.
   - Speaker—Phone is writing images to its flash memory.

4. The phone screen displays the Cisco Systems, Inc., logo screen.
5. These messages display as the phone starts:
   - Verifying load (if the phone load does not match the load on the TFTP server). If this message displays, the phone start up again and repeats step 1 through step 4 above.
   - Configuring IP.
   - Updating CTL.
   - Updating Locale.
   - Configuring Unified CM List.
   - Registering.
6. The main phone screen displays:
   - Current date and time
   - Primary directory number
   - Additional directory numbers and speed dial numbers, if configured
   - Softkeys

If the phone successfully passes through these stages, it has started up properly. If the phone does not start up properly, see the "Resolving Startup Problems" section on page 9-1.

Configuring Startup Network Settings

If you are not using DHCP in your network, you must configure these network settings on the Cisco Unified IP Phone after installing the phone on the network:

- IP address
- IP subnet information
- Default gateway IP address
- TFTP server IP address

You may also configure these optional settings as necessary:

- Domain name

- DNS server IP address

Collect this information and see the instructions in Chapter 4, "Configuring Settings on the Cisco Unified IP Phone."

Configuring Security on the Cisco Unified IP Phone

The security features protect against several threats, including threats to the identity of the phone and to data. These features establish and maintain authenticated communication streams between the phone and the Cisco Unified Communications Manager server, and digitally sign files before they are delivered.

For more information about the security features, see the "Understanding Security Features for Cisco Unified IP Phones" section on page 1-8. Also, refer to *Cisco Unified Communications Manager Security Guide*.

A Locally Significant Certificate (LSC) installs on phones after you perform the necessary tasks that are associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified Communications Manager Administration to configure an LSC, as described in *Cisco Unified Communications Manager Security Guide*.

Alternatively, you can initiate the installation of an LSC from the Security Configuration menu on the phone. This menu also lets you update or remove an LSC.

Before you begin, make sure that the appropriate Cisco Unified Communications Manager and the CAPF security configurations are complete:

- The CTL file should have a CAPF certificate.
- The CAPF certificate must exist in the /usr/local/cm/.security/certs folder in every server in the cluster.
- The CAPF is running and configured.

Refer to *Cisco Unified Communications Manager Security Guide* for more information.

To configure an LSC on the phone, perform the following procedure. Depending on how you have configured the CAPF, this procedure installs an LSC, updates an existing LSC, or removes an existing LSC.

Procedure

Step 1 Obtain the CAPF authentication code that was set when the CAPF was configured.

Step 2 From the phone, press the **Settings > Security Configuration**.

Note You can control access to the Settings Menu by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window. For more information, see *Cisco Unified Communications Manager Administration Guide*.

Step 3 Press ****#** to unlock settings on the Security Configuration menu. (See the "Unlocking and Locking Options" section on page 4-3 for information about using locking and unlocking options.)

Note If a Settings Menu password has been provisioned, SIP phones present an "Enter password" prompt after you enter **#.

Step 4 Scroll to LSC and press the **Update** softkey.

The phone prompts for an authentication string.

Step 5 Enter the authentication code and press the **Submit** softkey.

The phone begins to install, update, or remove the LSC, depending on how the CAPF was configured. During the procedure, a series of messages displays in the LSC option field in the Security Configuration menu so you can monitor progress. When the procedure completes successfully, the phone will display Installed or Not Installed.

The LSC install, update, or removal process can take a long time to complete. You can stop the process at any time by pressing the **Stop** softkey from the Security Configuration menu. (Settings must be unlocked before you can press this softkey.)

When the phone successfully completes the installation procedure, it displays "Success." If the phone displays, "Failure," the authorization string may be incorrect or the phone may not be enabled for upgrading. Refer to error messages generated by the CAPF and take appropriate actions.

You can verify that an LSC is installed on the phone by choosing **Settings > Model Information** and ensuring that the LSC setting shows Installed.

Related Topic

- Understanding Security Features for Cisco Unified IP Phones, page 1-8

CHAPTER 4

Configuring Settings on the Cisco Unified IP Phone

The Cisco Unified IP Phone includes many configurable network and device settings that you may need to modify before the phone is functional for your users. You can access these settings, and change many of them, through menus on the phone.

This chapter includes the following topics:

- Configuration Menus on the Cisco Unified IP Phone 7970 Series, page 4-1
- Overview of Options Configurable from a Phone, page 4-4
- Network Configuration Menu, page 4-5
- Device Configuration Menu, page 4-10
- Security Configuration Menu, page 4-29

Configuration Menus on the Cisco Unified IP Phone 7970 Series

The Cisco Unified IP Phone includes the following configuration menus:

- Network Configuration menu—Provides options for viewing and making a variety of network settings. For more information, see the "Network Configuration Menu" section on page 4-5.
- Device Configuration menu—Provides access to sub-menus from which you can view a variety of non network-related settings. For more information, see the "Device Configuration Menu" section on page 4-10.
- Security Configuration menu—Provides options for displaying and modifying security settings. For more information, see the "Security Configuration Menu" section on page 4-29.

Before you can change option settings on the Network Configuration menu, you must unlock options for editing. See the "Unlocking and Locking Options" section on page 4-3 for instructions.

For information about the keys you can use to edit or change option settings, see the "Editing Values" section on page 4-3.

You can control whether a phone user has access to phone settings by using the Settings Access field in Cisco Unified Communications Manager Administration Phone Configuration.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Unlocking and Locking Options, page 4-3

- Editing Values, page 4-3
- Overview of Options Configurable from a Phone, page 4-4
- Network Configuration Menu, page 4-5
- Device Configuration Menu, page 4-10
- Security Configuration Menu, page 4-29

Displaying a Configuration Menu

To display a configuration menu, perform the following steps.

Note You can control whether a phone has access to the Settings menu or to options on this menu by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone configuration window. The Settings Access field accepts these values:

- **Enabled**—Allows access to the Settings menu.
- **Disabled**—Prevents access to the Settings menu.
- **Restricted**—Allows access to the User Preferences menu and allows volume changes to be saved. Prevents access to other options on the Settings menu.

If you cannot access an option on the Settings menu, check the Settings Access field.

Procedure

Step 1 Press the **Settings** button to access the Settings menu.

Step 2 Perform one of these actions to display the desired menu:

- Use the **Navigation** button to select the desired menu and then press the **Select** softkey.
- Use the keypad on the phone to enter the number that corresponds to the menu.

Step 3 To display a submenu, repeat Step 2.

Step 4 To exit a menu, press the **Exit** softkey.

Related Topics

- Unlocking and Locking Options, page 4-3
- Editing Values, page 4-3
- Overview of Options Configurable from a Phone, page 4-4
- Network Configuration Menu, page 4-5
- Device Configuration Menu, page 4-10
- Security Configuration Menu, page 4-29

Unlocking and Locking Options

Configuration options that can be changed from a phone are locked by default to prevent users from making changes that could affect the operation of a phone. You must unlock these options before you can change them.

When options are inaccessible for modification, a *locked* padlock icon appears on the configuration menus. When options are unlocked and accessible for modification, an *unlocked* padlock icon appears on these menus.

To unlock or lock options, press ****#**. This action either locks or unlocks the options, depending on the previous state.

Note If a Settings Menu password has been provisioned, SIP phones present an "Enter password" prompt after you enter **#.

Make sure to lock options after you have made your changes.

Caution Do not press ****#** to unlock options and then immediately press ****#** again to lock options. The phone will interpret this sequence as ****#****, which will reset the phone. To lock options after unlocking them, wait at least 10 seconds before you press ****#** again.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Editing Values, page 4-3
- Overview of Options Configurable from a Phone, page 4-4
- Network Configuration Menu, page 4-5
- Device Configuration Menu, page 4-10

Editing Values

When you edit the value of an option setting, follow these guidelines:

- Use the keys on the keypad to enter numbers and letters.
- To enter letters by using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the **2** key once for "a," twice quickly for "b," and three times quickly for "c." After you pause, the cursor automatically advances to allow you to enter the next letter.
- To enter a period (for example, in an IP address), press the **.** (period) softkey or press ***** on the keypad.
- Press the **<<** softkey if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press the **Cancel** softkey before pressing the **Save** softkey to discard any changes that you have made.

Note The Cisco Unified IP Phone provides several methods you can use to reset or restore option settings, if necessary. For more information, see the "Resetting or Restoring the Cisco Unified IP Phone" section on page 9-13.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Unlocking and Locking Options, page 4-3
- Overview of Options Configurable from a Phone, page 4-4
- Network Configuration Menu, page 4-5
- Device Configuration Menu, page 4-10
- Security Configuration Menu, page 4-29

Overview of Options Configurable from a Phone

The settings that you can change on a phone fall into several categories, as shown in Table 4-1. For a detailed explanation of each setting and instructions for changing them, see the "Network Configuration Menu" section on page 4-5.

Note There are several options on various configuration menus that are for display only or that you can configure from Cisco Unified Communications Manager. These options also are also described in this chapter.

Table 4-1 Settings Configurable from the Phone

Category	Description	Network Configuration Menu Option
General Network Settings		
VLAN settings	Admin. VLAN ID allows you to change the administrative VLAN used by the phone. PC VLAN allows the phone to interoperate with third-party switches that do not support a voice VLAN.	Admin. VLAN ID PC VLAN
Port settings	Allow you to set the speed and duplex of the network and access ports.	SW Port Configuration PC Port Configuration
IPv4 Network Settings		
DHCP settings	Dynamic Host Configuration Protocol (DHCP) automatically assigns IP address to devices when you connect them to the network. Cisco Unified IP Phones enable DHCP by default.	DHCP DHCP Address Released

Table 4-1 Settings Configurable from the Phone (continued)

Category	Description	Network Configuration Menu Option
IP settings	If you do not use DHCP in your network, you can make IP settings manually.	Domain Name
		IP Address
		Subnet Mask
		Default Router 1-5
		DNS Server 1-5
TFTP settings	If you do not use DHCP to direct the phone to a TFTP server, you must manually assign a TFTP server. You can also assign an alternative TFTP server to use instead of the one assigned by DHCP.	TFTP Server 1
		Alternate TFTP
		TFTP Server 2

Related Topics

- Displaying a Configuration Menu, page 4-2
- Unlocking and Locking Options, page 4-3
- Editing Values, page 4-3
- Network Configuration Menu, page 4-5
- Device Configuration Menu, page 4-10

Network Configuration Menu

The Network Configuration menu provides options for viewing and making a variety of network settings. Table 4-2 and Table 4-3 describe these options and, where applicable, explains how to change them.

For information about how to access the Network Configuration menu, see the "Displaying a Configuration Menu" section on page 4-2.

Note The phone also has a Network Configuration menu that you access directly from the Settings menu. For information about the options on that menu, see the "Network Configuration" section on page 4-25.

Before you can change an option on this menu, you must unlock options as described in the "Unlocking and Locking Options" section on page 4-3. The **Edit**, **Yes**, or **No** softkeys for changing network configuration options appear only if options are unlocked.

For information about the keys you can use to edit options, see the "Editing Values" section on page 4-3.

Table 4-2 Network Configuration Menu Options

Option	Description	To Change
IPv4 Configuration	In the IPv4 Configuration menu, you can do the following: • Enable or disable the phone to use the IP address that is assigned by the DHCP server. • Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers. For more information on the IPv4 address fields, refer to Table 4-3.	1. Unlock network configuration options. 2. Scroll to IPv4 Configuration and press the **Select** softkey.
IPv6 Configuration	This menu setting is disabled in this release.	
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only—Cannot configure.
Host Name	Unique host name that the DHCP server assigned to the phone.	Display only—Cannot configure.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to **No**. 3. Scroll to the Domain Name option, press the **Edit** softkey, and then enter a new domain name. 4. Press the **Validate** softkey and then press the **Save** softkey.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member. If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN. If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option is blank.	The phone obtains its Operational VLAN ID via Cisco Discovery Protocol (CDP) from the switch to which the phone is attached. To assign a VLAN ID manually, use the Admin VLAN ID option.
Admin. VLAN ID	Auxiliary VLAN in which the phone is a member. Used only if the phone does not receive an auxiliary VLAN from the switch; otherwise it is ignored.	1. Unlock network configuration options. 2. Scroll to the Admin. VLAN ID option, press the **Edit** softkey, and then enter a new Admin VLAN setting. 3. Press the **Validate** softkey and then press the **Save** softkey.

Table 4-2 Network Configuration Menu Options (continued)

Option	Description	To Change
SW Port Configuration	Speed and duplex of the network port (labeled 10/100 SW on the Cisco Unified IP Phone 7970, and 10/100/1000 SW on the Cisco Unified IP Phone 7971G-GE). Valid values: • Auto Negotiate • 10 Half—10-BaseT/half duplex • 10 Full—10-BaseT/full duplex • 100 Half—100-BaseT/half duplex • 100 Full—100-BaseT/full duplex • 1000 Full—1000-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the PC Port Configuration option to the same setting.	1. Unlock network configuration options. 2. Scroll to the SW Port Configuration option and then press the **Edit** softkey. 3. Scroll to the setting that you want and then press the **Select** softkey. 4. Press the **Save** softkey.
PC Port Configuration	Speed and duplex of the access port (labeled 10/100 PC on the Cisco Unified IP Phone 7970, and 10/100/1000 PC on the Cisco Unified IP Phone 7971G-GE). Valid values: • Auto Negotiate • 10 Half—10-BaseT/half duplex • 10 Full—10-BaseT/full duplex • 100 Half—100-BaseT/half duplex • 100 Full—100-BaseT/full duplex • 1000 Full—1000-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the SW Port Configuration option to the same setting.	1. Unlock network configuration options. 2. Scroll to the PC Port Configuration option and then press the **Edit** softkey. 3. Scroll to the setting that you want and then press the **Select** softkey. 4. Press the **Save** softkey.
PC VLAN	Allows the phone to interoperate with 3rd party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before you can change this option.	1. Unlock network configuration options. 2. Make sure the Admin VLAN ID option is set. 3. Scroll to the **PC VLAN** option, press the **Edit** softkey, and then enter a new PC VLAN setting. 4. Press the **Validate** softkey and then press the **Save** softkey.

Table 4-3 IPv4 Configuration Menu Options

Option	Description	To Change
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.	Display only—Cannot configure.
IP Address	Internet Protocol (IP) address of the phone. If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to **No**. 3. Scroll to the IP Address option, press the **Edit** softkey, and then enter a new IP Address. 4. Press the **Validate** softkey and then press the **Save** softkey.
Subnet Mask	Subnet mask used by the phone.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to **No.** 3. Scroll to the Subnet Mask option, press the **Edit** softkey, and then enter a new subnet mask. 4. Press the **Validate** softkey and then press the **Save** softkey.
Default Router 1 Default Router 2 Default Router 3 Default Router 4 Default Router 5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5).	1. Unlock network configuration options. 2. Set the DHCP Enabled option to **No.** 3. Scroll to the appropriate Default Router option, press the **Edit** softkey, and then enter a new router IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup routers. 6. Press the **Save** softkey.
DNS Server 1 DNS Server 2 DNS Server 3 DNS Server 4 DNS Server 5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to **No.** 3. Scroll to the appropriate DNS Server option, press the **Edit** softkey, and then enter a new DNS server IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup DNS servers. 6. Press the **Save** softkey.
DHCP	Indicates whether the phone has DHCP enabled or disabled. When DHCP is enabled, the DHCP server assigns the phone an address. When DHCP is disabled, the administrator must manually assign an IP address to the phone.	1. Unlock network configuration options. 2. Scroll to the DHCP Enabled option and press the **No** softkey to disable DHCP, or press the **Yes** softkey to enable DHCP. 3. Press the **Save** softkey.

Table 4-3 IPv4 Configuration Menu Options (continued)

Option	Description	To Change
DHCP Address Released	Releases the IP address assigned by DHCP.	1. Unlock network configuration options. 2. Scroll to the DHCP Address Released option and press the **Yes** softkey to release the IP address assigned by DHCP, or press the **No** softkey if you do not want to release this IP address. 3. Press the **Save** softkey.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.	1. Unlock network configuration options. 2. Scroll to the Alternate TFTP option and press the **Yes** softkey if the phone should use an alternative TFTP server. 3. Press the **Save** softkey.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to yes, you must enter a non-zero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 1 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 1 option. A new CTL file will be downloaded from the new TFTP Server 1 address. For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, see the "Security Configuration Menu" section on page 4-29.	1. Unlock the CTL file if necessary (for example, if you are changing the administrative domain of the phone). 2. If DHCP is enabled, set the Alternate TFTP option to **Yes.** 3. Scroll to the TFTP Server 1 option, press the **Edit** softkey, and then enter a new TFTP server IP address. 4. Press the **Validate** softkey, and then press the **Save** softkey. **Note** If you forgot to unlock the CTL file, you can change the TFTP Server 1 address in the CTL file, then erase the CTL file by pressing the Erase softkey from the Security Configuration menu. A new CTL file will be downloaded from the new TFTP Server 1 address.

Table 4-3 IPv4 Configuration Menu Options (continued)

Option	Description	To Change
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 2 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 2 option. A new CTL file will be downloaded from the new TFTP Server 2 address. For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, see to the "Security Configuration Menu" section on page 4-29.	1. Unlock the CTL file, if necessary (for example, if you are changing the administrative domain of the phone). 2. Unlock network configuration options. 3. Enter an IP address for the TFTP Server 1 option. 4. Scroll to the TFTP Server 2 option, press the **Edit** softkey, and then enter a new backup TFTP server IP address. 5. Press the **Validate** softkey, and then press the **Save** softkey. **Note** If you forgot to unlock the CTL file, you can change the TFTP Server 2 address in the CTL file, then erase the CTL file by pressing the Erase softkey from the Security Configuration menu. A new CTL file will be downloaded from the new TFTP Server 2 address.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server instead of from a DHCP server.	Display only—Cannot configure.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Unlocking and Locking Options, page 4-3
- Editing Values, page 4-3
- Overview of Options Configurable from a Phone, page 4-4
- Device Configuration Menu, page 4-10

Device Configuration Menu

The Device Configuration menu provides access to nine sub-menus from which you can view a variety of settings that are specified in the configuration file for a phone. (The phone downloads the configuration file from the TFTP server.) These sub-menus are:

- Unified CM Configuration, page 4-11
- SIP Configuration Menu (SIP Phones Only), page 4-12
- Call Preferences Menu (SIP Phones Only), page 4-14
- HTTP Configuration Menu, page 4-15
- Locale Configuration Menu, page 4-16
- UI Configuration Menu, page 4-17

- Media Configuration Menu, page 4-19
- Power Save Configuration Menu, page 4-22
- Ethernet Configuration Menu, page 4-23
- Security Configuration Menu, page 4-23
- QoS Configuration Menu, page 4-25
- Network Configuration, page 4-25

For instructions about how to access the Device Configuration menu and its sub-menus, see the "Displaying a Configuration Menu" section on page 4-2.

Unified CM Configuration

The Unified CM Configuration contains the options Unified CM1, Unified CM 2, Unified CM3, Unified CM4, and Unified CM5. These options show Cisco Unified Communications Manager servers that are available for processing calls from the phone, in prioritized order. To change these options, use Cisco Unified Communications Manager Administration, Cisco Unified CM Group Configuration.

For an available Cisco Unified Communications Manager server, an option on the Unified CM Configuration will show the Cisco Unified Communications Manager server IP address or name and one of the states shown in Table 4-4.

Table 4-4 Cisco Unified Communications Manager Server States

State	Description
Active	Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services
Standby	Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable
Blank	No current connection to this Cisco Unified Communications Manager server

An option may also display one of more of the designations or icons shown in Table 4-5:

Table 4-5 Cisco Unified Communications Manager Server Designations

Designation	Description
SRST	Indicates a Survivable Remote Site Telephony router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. For more information, refer to *Cisco Unified Communications Manager Administration Guide*. You configure an SRST router address in the Cisco Unified Communications Manager Administration SRST Reference Configuration window (choose **System > SRST**). You configure an SRST reference in the Device Pool Configuration window (choose **System > Device Pool**).
TFTP	Indicates that the phone was unable to register with a Cisco Unified Communications Manager listed in its configuration file and that it registered with the TFTP server instead.
 (Authentication icon)	Indicates that the connection to the Cisco Unified Communications Manager is authenticated. For more information about authentication, refer to *Cisco Unified Communications Manager Security Guide*.
 (Encryption icon)	Indicates that the connection to the Cisco Unified Communications Manager is authenticated and encrypted. For more information about authentication and encryption, refer to *Cisco Unified Communications Manager Security Guide*. The Encryption icon is also displayed when a Cisco Unified IP phone is configured as *protected*. For more information about protected calls, refer to *Cisco Unified Communications Manager Security Guide*. Protected calls are not authenticated.

SIP Configuration Menu (SIP Phones Only)

The SIP Configuration menu is available on SIP phones. This menu contains these sub-menus:

- SIP General Configuration Menu, page 4-13
- Line Settings Menu (SIP Phones Only), page 4-14

SIP General Configuration Menu

The SIP General Configuration menu displays information about the configurable SIP parameters on a SIP phone. Table 4-6 describes the options in this menu.

Table 4-6 SIP General Configuration Menu Options

Option	Description	To Change
Preferred CODEC	Displays the CODEC to use when a call is initiated. This value will always be set to none.	Display only—cannot configure.
Out of Band DTMF	Displays the configuration of the out-of-band signaling (for tone detection on the IP side of a gateway). The Cisco Unified IP Phone (SIP) supports out-of-band signaling by using the AVT tone method. This value will always be set to avt.	Display only—cannot configure.
Register with Proxy	Displays if the phone must register with a proxy server during initialization. This value will always be set to Yes.	Display only—cannot configure.
Register Expires	Displays the amount of time, in seconds, after which a registration request expires.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
Phone Label	Displays the text that is displayed on the top right status line of the LCD on the phone. This text is for end-user display only and has no effect on caller identification or messaging. This value will always be set to null.	Display only—cannot configure.
Enable VAD	Displays if voice activation detection (VAD) is enabled. This value is set to No by default.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
Start Media Port	Displays the start Real-Time Transport Protocol (RTP) range for media.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
End Media Port	Displays the end Real-Time Transport Protocol (RTP) range for media.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
NAT Enabled	Displays if Network Address Translation (NAT) is enabled. This value will always be set to false.	Display only—cannot configure.
NAT Address	Displays the WAN IP address of the NAT or firewall server. This value will always be set to null.	Display only—cannot configure.
Call Statistics	Displays if call statistics are enabled on the phone.This value is set to No by default.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Device Configuration Menu, page 4-10

Line Settings Menu (SIP Phones Only)

The Line Settings menu displays information that relates to the configurable parameters for each of the lines on a SIP phone. Table 4-7 describes the options in this menu.

Table 4-7 Line Settings Menu Options

Option	Description	To Change
Name	Displays the lines and the number used to register each line.	Use Cisco Unified Communications Manager Administration to modify.
Short Name	Displays the short name configured for the line.	Use Cisco Unified Communications Manager Administration to modify.
Authentication Name	Displays the name used by the phone for authentication if a registration is challenged by the call control server during initialization.	Use Cisco Unified Communications Manager Administration to modify.
Display Name	Displays the identification the phone uses for display for caller identification purposes.	Use Cisco Unified Communications Manager Administration to modify.
Proxy Address	The value is left blank because it is not applicable to SIP phones that are using Cisco Unified Communications Manager.	Display only—Cannot configure.
Proxy Port	The value is left blank because it is not applicable to SIP phones that are using Cisco Unified Communications Manager.	Display only—Cannot configure.
Shared Line	Displays if the line is part of a shared line (Yes) or not (No).	Display only—Cannot configure.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Device Configuration Menu, page 4-10

Call Preferences Menu (SIP Phones Only)

The Call Preferences menu displays settings that relate to the settings for the call preferences on a SIP phone. Table 4-8 describes the options in this menu.

Table 4-8 Call Preferences Menu Options

Option	Description	To Change
Caller ID Blocking	Indicates whether caller ID blocking is enabled (Yes) or disabled (No) for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
Anonymous Call Block	Indicates whether anonymous call block is enabled (Yes) or disabled (No) for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
Call Waiting Preferences	Displays a sub-menu that indicates whether call waiting is enabled (Yes) or disabled (No) for each line.	From Cisco Unified Communications Manager Administration, choose **Call Routing > Directory Number**.

Table 4-8 Call Preferences Menu Options (continued)

Option	Description	To Change
Call Hold Ringback	Indicates whether the call hold ringback feature is enabled (Yes) or disabled (No) for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
Stutter Msg Waiting	Indicates whether stutter message waiting is enabled (Yes) or disabled (No) for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
Call Logs BLF Enabled	Indicates whether BLF for call logs is enabled (Yes) or disabled (No) for the phone.	Use Cisco Unified Communications Manager Administration.
Auto Answer Preferences	Displays a sub-menu that indicates whether auto answer is enabled (Yes) or disabled (No) for the each line.	From Cisco Unified Communications Manager Administration, choose **Call Routing > Directory Number**.
Speed Dials	Displays a sub-menu that displays the lines available on the phone. Select a line to see the speed dial label and number assigned to that line.	From Cisco Unified Communications Manager Administration, choose **Device > Add a New Speed Dial**.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Device Configuration Menu, page 4-10

HTTP Configuration Menu

The HTTP Configuration menu displays the URLs of servers from which the phone obtains a variety of information. This menu also displays information about the idle display on the phone.

Table 4-9 describes the options on the HTTP Configuration menu.

Table 4-9 HTTP Configuration Menu Options

Option	Description	To Change
Directories URL	URL of the server from which the phone obtains directory information.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Messages URL	URL of the server from which the phone obtains message services.	Use Cisco Unified Communications Manager Administration to modify **> Device > Phone > Phone Configuration**.
Information URL	URL of the help text that appears on the phone.	From Cisco Unified Communications Manager Administration, choose **> Device > Phone > Phone Configuration**.

Table 4-9 HTTP Configuration Menu Options (continued)

Option	Description	To Change
Authentication URL	URL that the phone uses to validate requests made to the phone web server.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Proxy Server URL	URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the phone HTTP client and provides responses from the non-local host to the phone HTTP client.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Idle URL	URL of an XML service that the phone displays when the phone has not been used for the time specified in the Idle URL Time option and no menu is open. For example, you could use the Idle URL option and the Idle URL Timer option to display a stock quote or a calendar on the LCD screen when the phone has not been used for 5 minutes.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Idle URL Time	Number of seconds that the phone has not been used and no menu is open before the XML service specified in the Idle URL option is activated.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Locale Configuration Menu

The Locale Configuration menu displays information about the user locale and the network locale used by the phone. Table 4-10 describes the options on this menu.

Table 4-10 Locale Configuration Menu Options

Option	Description	To Change
User Locale	User locale associated with the phone user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
User Locale Version	Version of the user locale loaded on the phone.	Display only—Cannot configure.
User Locale Char Set	Character set that the phone uses for the user locale.	Display only—Cannot configure.
Network Locale	Network locale associated with the phone user. The network locale identifies a set of detailed information that supports the phone in a specific location, including definitions of the tones and cadences used by the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Table 4-10 Locale Configuration Menu Options (continued)

Option	Description	To Change
Network Locale Version	Version of the network locale loaded on the phone.	Display only—Cannot configure.
NTP Configuration (SIP phones only)	Provides access to the NTP Configuration Menu. For more information, see the "NTP Configuration Menu (SIP Phones Only)" section on page 4-17	Display only—Cannot configure.

NTP Configuration Menu (SIP Phones Only)

The NTP Configuration menu displays information about the NTP server and mode configuration used by SIP phones. Table 4-11 describes the options on this menu.

Table 4-11 NTP Configuration Menu Options

Option	Description	To Change
NTP Server 1	IP address of the primary NTP server.	Display only—Cannot configure.
NTP Server 2	IP address of the secondary or backup NTP server.	Display only—Cannot configure.
NTP Mode 1	Primary server mode. Supported modes are Directed Broadcast and Unicast.	Display only—Cannot configure.
NTP Mode 2	Secondary server mode. Supported modes are Directed Broadcast and Unicast.	Display only—Cannot configure.

UI Configuration Menu

The UI Configuration menu displays the status of various user interface features on the phone. Table 4-12 describes the options on this menu.

Table 4-12 UI Configuration Menu Options

Option	Description	To Change
Auto Line Select	Indicates whether the phone shifts the call focus to incoming calls on all lines. When this option is disabled, the phone only shifts the call focus to incoming calls on the line that is in use. When this option is enabled, the phone shifts the call focus to the line with the most recent incoming call. Default: Disabled	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
BLF for Call Lists	Indicates whether the Busy Lamp Field (BLF) is enabled for call lists.	From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.

Table 4-12 UI Configuration Menu Options (continued)

Option	Description	To Change
Reverting Focus Priority	Indicates whether the phone shifts the call focus on the phone screen to an incoming call or a reverting hold call. Settings include: **Lower**—Focus priority given to incoming calls. **Higher**—Focus priority given to reverting calls. **Even**—Focus priority given to the first call.	From Cisco Unified Communications Manager Administration, choose **System > Device Pool**. See also: Hold Reversion.
Auto Call Select	Indicates whether the phone automatically shifts the call focus to an incoming call on the same line when the user is already on a call. When this option is enabled, the phone shifts the call focus to the most recent incoming call. When this option is disabled, all automatic focus changes, including Auto Line Select, are disabled regardless of their setting. Default: Enabled	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
"more" Softkey Timer	Indicates the number of seconds that additional softkeys are displayed after the user presses **more**. If this timer expires before the user presses another softkey, the display reverts to the initial softkeys. Range: 5 to 30; 0 represents an infinite timer. Default: 5	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Wideband Headset UI Control	Indicates whether the user can configure the Wideband Headset option in the phone user interface. Values: • Enabled—The user can configure the Wideband Headset option in the Audio Preferences menu on the phone (choose **> User Preferences > Audio Preferences> Wideband Headset**). • Disabled—The value of the Wideband Headset option in Cisco Unified Communications Manager Administration gets used (see Media Configuration Menu, page 4-19) Default: Enabled	Use Cisco Unified Communications Manager Administration **> Device > Phone > Phone Configuration**.

Table 4-12 UI Configuration Menu Options (continued)

Option	Description	To Change
Wideband Handset UI Control	Indicates whether the user can configure the Wideband Handset option in the phone user interface. Values: • Enabled—The user can configure the Wideband Handset option in the Audio Preferences menu on the phone (choose **> User Preferences > Audio Preferences> Wideband Handset**). • Disabled—The value of the Wideband Handset option in Cisco Unified Communications Manager Administration gets used (see Media Configuration Menu, page 4-19**).** Default: Enabled	Use Cisco Unified Communications Manager Administration > Device > Phone > Phone Configuration.
Personalization	Indicates whether the phone has been enabled for configuring custom ring tones and wallpaper images. Default: Enabled	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Single Button Barge	Indicates whether the Single Button Barge feature is enabled for the phone. Default: Disabled.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Media Configuration Menu

The Media Configuration menu displays whether the headset, speakerphone, and video capability (SCCP phones only) are enabled on the phone. This menu also displays options for recording tones that the phone may play to indicate that a call may be recorded. Table 4-13 describes the options on this menu.

Table 4-13 Media Configuration Menu Options

Option	Description	To Change
Headset Enabled	Indicates whether the **Headset** button is enabled on the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Video Capability Enabled (SCCP phones only)	Indicates whether the phone can participate in video calls when connected to an appropriately equipped computer.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Table 4-13 Media Configuration Menu Options (continued)

Option	Description	To Change
Recording Tone	Indicates whether a recording tone (often referred to as a *beep tone*) is enabled or disabled for the phone. If the recording tone option is enabled, the phone plays the beep tone in both directions of every call, regardless of whether the call actually gets recorded. The beep tone first sounds when a call is answered. You may want to notify your users if you enable this option. Default: Disabled Related Parameters: • Recording Tone Local Volume • Recording Tone Remote Volume • Recording Tone Duration Other related parameters—Beep tone frequency in hz, the length of the beep tone (called *duration*), and how often the beep tone plays (called *interval*)—are defined on a per-Network Locale basis in the xml file that defines tones. This xml file is usually named tones.xml or g3-tones.xml.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Recording Tone Local Volume	Indicates the loudness setting for the beep tone that is received by the party whose phone has the Recording Tone option enabled. This setting applies for each listening device (handset, speakerphone, headset). Range: 0 percent (no tone) to 100 percent (same level as current volume setting on the phone). Default: 100 See also: Recording Tone	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Recording Tone Remote Volume	Indicates the loudness setting for the beep tone that the *remote party* receives. The *remote party* is the party who is on a call with the party whose phone has the Recording Tone option enabled. Range: 0 percent to 100 percent. (0 percent is –66 dBM and 100 percent is –3 dBM.) Default: 84 percent (–10dBM) See also: Recording Tone	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Table 4-13 Media Configuration Menu Options (continued)

Option	Description	To Change
Recording Tone Duration	Indicates the length of time in milliseconds that the beep tone plays. If the value you configure here is less than one third the interval, then this value overrides the default provided by the Network Locale. Range: 0 to 3000 **Note** For some Network Locales that use a complex cadence, this setting applies only to the first beep tone. See also: Recording Tone	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Wideband Headset	Indicates whether wideband is enabled or disabled for the headset. Default: Disabled	• If Wideband Headset UI Control is enabled, you or the user can use the phone and choose > **User Preferences > Audio Preferences > Wideband Headset**. • If Wideband Headset UI Control is disabled, from Cisco Unified Communications Manager Administration and choose **Device > Phone > Phone Configuration** to set this value. **Note** If you allowed this option to be user controllable (in the Wideband Headset UI Control option), the user-configured value takes precedence.
Wideband Handset	Indicates whether wideband is enabled or disabled for the handset. Default: "Use Phone Default" on Cisco Unified Communications Manager Administration. (This default means that the phone will be enabled for a wideband handset only if the phone was shipped with a wideband handset.)	• If Wideband Handset UI Control is enabled, you or the user can choose > **User Preferences > Audio Preferences > Wideband Handset.** • If Wideband Handset UI Control is disabled, use Cisco Unified Communications Manager Administration and choose **Device > Phone > Phone Configuration** to set this value. **Note** If you allowed this option to be user controllable (in the Wideband Handset UI Control option), the user-configured value takes precedence.

Table 4-13 Media Configuration Menu Options (continued)

Option	Description	To Change
Enterprise Advertise G.722 Codec	Enables/disables Cisco Unified IP Phones to advertise the G.722 codec to Cisco Unified Communications Manager. If enabled (default), and if each endpoint in the attempted call supports G.722 in its capabilities set, Cisco Unified Communications Manager will choose G.722 for the call. **Note** When a phone is registered with a Cisco Unified Communications Manager that does not support this setting, the default is "Disabled."	From Cisco Unified Communications Manager Administration and choose **System > Enterprise Parameters.**
Device Advertise G.722 Codec	Allows you to override the Enterprise Advertise G.722 Codec on a per-phone basis. The default is "Use System Default," which means the value configured for the Enterprise Advertise G.722 Codec parameter gets used.	From Cisco Unified Communications Manager Administration and choose **Device > Phone.**

Power Save Configuration Menu

The Power Save Configuration menu displays the settings that control when the LCD screen on a phone turns off to conserve power. Table 4-14 describes the options on this menu.

For detailed information about configuring these settings, see the "Automatically Disabling the Cisco Unified IP Phone Touchscreen" section on page 6-7.

Table 4-14 Power Save Configuration Menu Options

Option	Description	To Change
Display On Time	Time each day that the LCD screen turns on automatically (except on the days specified in the Days Display Not Active field).	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Display On Duration	Length of time that the LCD screen remains on after turning on at the time shown in the Display On Time option.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Display Idle Timeout	Length of time that the phone is idle before the display turns off. Applies only when the display was off as scheduled and was turned on by an end-user (by pressing a button on the phone, touching the touchscreen, or lifting the handset).	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Days Display Not Active	Days that the display does not turn on automatically at the time specified in the Display On Time option.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Display On When Incoming Call	Indicates whether the LCD screen automatically illuminates when a call is received.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Ethernet Configuration Menu

The Ethernet Configuration menu includes the options that are described in Table 4-15.

Table 4-15 Ethernet Configuration Menu Option

Option	Description	To Change
Forwarding Delay	Indicates whether the internal switch begins forwarding packets between the PC port and switched port on the phone when the phone becomes active. • When forwarding delay is set to disabled, the internal switch begins forwarding packets immediately. • When forwarding delay is set to enabled, the internal switch waits 8 seconds before forwarding packets between the PC port and the switch port. Default is disabled.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Span to PC Port	Indicates whether the phone will forward packets transmitted and received on the network port to the access port. Enable this option if an application that requires monitoring of the phone's traffic is being run on the access port. These applications include monitoring and recording applications (common in call center environments) and network packet capture tools that are used for diagnostic purposes.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Security Configuration Menu

The Security Configuration menu that you display from the Device Configuration menu displays settings that relate to security for the phone.

Note The phone also has a Security Configuration menu that you access directly from the Settings menu. For information about the security options on that menu, see the "Security Configuration Menu" section on page 4-29.

Table 4-16 describes the options on the Security Configuration menu.

Table 4-16 Security Configuration Menu Options

Option	Description	To Change
PC Port Disabled	Indicates whether the access port on the phone is enabled or disabled. **Note** If disabled, video will not work on this phone, even if video is enabled.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous Address Resolution Protocol (ARP) responses. Disabling the phone's ability to accept Gratuitous ARP will prevent applications that use this mechanism to monitor and record voice streams from working. If voice monitoring is not desired, set this option to No (disabled).	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Voice VLAN Enabled	Indicates whether the phone allows a device attached to the access port to access the Voice VLAN. Setting this option to No (disabled) prevents the attached PC from sending and receiving data on the Voice VLAN. This setting also prevents the PC from receiving data sent and received by the phone. Set this setting to Yes (enabled) if an application that requires monitoring of the phone's traffic is running on the PC. These applications include monitoring and recording applications and network monitoring software.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Security Mode	Displays the security mode that is set for the phone.	Use Cisco Unified Communications Manager Administration to modify.
Logging Display	For use by the Cisco Technical Assistance Center (TAC), if necessary.	

QoS Configuration Menu

The QoS Configuration menu displays information that relates to quality of service (QoS) for the phone. Table 4-17 describes the options on this menu.

Table 4-17 QoS Configuration Menu Options

Option	Description	To Change
DSCP For Call Control	Differentiated Services Code Point (DSCP) IP classification for call control signaling.	From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
DSCP For Configuration	DSCP IP classification for any phone configuration transfer.	From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
DSCP For Services	DSCP IP classification for phone-based services.	From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Network Configuration Menu, page 4-5

Network Configuration

The Network Configuration menu displays device-specific network configuration settings on the phone. Table 4-18 describes the options in this menu.

Note The phone also has a Network Configuration menu that you access directly from the Settings menu. For information about the options on that menu, see the "Network Configuration Menu" section on page 4-5.

Table 4-18 Network Configuration Menu Options

Option	Description	To Change
Load Server	Used to optimize installation time for phone firmware upgrades and offload the WAN by storing images locally, negating the need to traverse the WAN link for each phone's upgrade. You can set the Load Server to another TFTP server IP address or name (other than the TFTP Server 1 or TFTP Server 2) from which the phone firmware can be retrieved for phone upgrades. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade. **Note** The Load Server option allows you to specify an alternate TFTP server for phone upgrades only. The phone continues to use TFTP Server 1 or TFTP Server 2 to obtain configuration files. The Load Server option does not provide management of the process and of the files, such as file transfer, compression, or deletion.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
RTP Control Protocol	Indicates whether the phone supports the Real-Time Control Protocol (RTCP). Settings include: • Enabled • Disabled—default If this feature is disabled, several call statistic values display as 0. For additional information, see the following sections: • Call Statistics Screen, page 7-13 • Streaming Statistics, page 8-10	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Table 4-18 Network Configuration Menu Options (continued)

Option	Description	To Change
Peer Firmware Sharing	The Peer Firmware Sharing feature provides these advantages in high speed campus LAN settings: • Limits congestion on TFTP transfers to centralized TFTP servers • Eliminates the need to manually control firmware upgrades • Reduces phone downtime during upgrades when large numbers of devices are reset simultaneously Peer Firmware Sharing may also aid in firmware upgrades in branch/remote office deployment scenarios over bandwidth-limited WAN links. When enabled, it allows the phone to discover like phones on the subnet that are requesting the files that make up the firmware image, and to automatically assemble transfer hierarchies on a per-file basis. The individual files making up the firmware image are retrieved from the TFTP server by only the root phone in the hierarchy, and are then rapidly transferred down the transfer hierarchy to the other phones on the subnet using TCP connections This menu option indicates whether the phone supports peer to peer image distribution. Settings include: • Enabled • Disabled—default	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Log Server	Indicates the IP address and port of the remote logging machine to which the phone sends log messages. These log messages help in debugging the peer to peer image distribution feature. **Note** The remote logging setting does not affect the sharing log messages sent to the phone log.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
CDP: PC Port	Indicates whether CDP is enabled on the PC port (default is enabled). Enable CDP on the PC port when Cisco VT Advantage/Unified Video Advantage (CVTA) is connected to the PC port. CVTA does not work without CDP interaction with the phone. **Note** When CDP is disabled in Cisco Unified Communications Manager, a warning is displayed, indicating that disabling CDP on the PC port prevents CVTA from working. The current PC and switch port CDP values are shown on the Settings menu.	From Cisco Unified Communications Manager Administration, choose **Device > Phone**.

Table 4-18 Network Configuration Menu Options (continued)

Option	Description	To Change
CDP: SW Port	Indicates whether CDP is enabled on the switch port (default is enabled). • Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security. • Enable CDP on the switch port when the phone is connected to a Cisco switch. **Note** When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, indicating that CDP should be disabled on the switch port only if the phone is connected to a non-Cisco switch. The current PC and switch port CDP values are shown on the Settings menu.	From Cisco Unified Communications Manager Administration, choose **Device > Phone**.
LLDP: PC Port	Enables and disables Link Layer Discovery Protocol (LLDP) on the PC port. Use this setting to force the phone to use a specific discovery protocol. Settings include: • Enabled—default • Disabled	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**
LLDP-MED: SW Port	Enables and disables Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) on the switch port. Use this setting to force the phone to use a specific discovery protocol, which should match the protocol supported by the switch. Settings include: • Enabled—default • Disabled	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**
LLDP Power Priority	Advertises the phone's power priority to the switch, enabling the switch to appropriately provide power to the phones. Settings include: • Unknown—default • Low • High • Critical	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**
LLDP Asset ID	Identifies the asset ID assigned to the phone for inventory management.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**

Related Topics

- Displaying a Configuration Menu, page 4-2
- Network Configuration Menu, page 4-5

Security Configuration Menu

The Security Configuration that you access directly from the Settings menu provides information about various security settings. It also provides access to the CTL File menu and the Trust List menu, if a CTL file is installed on the phone.

For information about how to access the Security Configuration menu and its sub-menus, see the "Displaying a Configuration Menu" section on page 4-2.

Note The phone also has a Security Configuration menu that you access from the Device menu. For information about the security options on that menu, see the "Security Configuration Menu" section on page 4-23.

Table 4-19 describes the options in the security configuration menu.

Table 4-19 Security Menu Settings

Option	Description	To Change
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Security Mode	Displays the security mode that is set for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
MIC	Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the MIC for your phone, refer to the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified Communications Manager Security Guide*.
LSC	Indicates whether a locally significant certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the LSC for your phone, refer to the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified Communications Manager Security Guide*.
CTL File	Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone. If no CTL file is installed on the phone, this field displays No. (If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets.	For more information about this file, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified Communications Manager Security Guide*. If a CTL file is installed on the phone, also provides access to the CTL File screen. For more information, see the "CTL File Menu" section on page 4-30.
Trust List	If a CTL file is installed on the phone, provides access to the Trust List menu.	For more information, see the "Trust List Menu" section on page 4-31.
CAPF Server	Displays the IP address and the port of the CAPF server that the phone uses.	For more information about this server, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified Communications Manager Security Guide*.

Table 4-19 Security Menu Settings (continued)

Option	Description	To Change
802.1X Authentication	Allows you to enable 802.1X authentication for this phone.	See the "802.1X Authentication and Status" section on page 4-31.
802.1X Authentication Status	Displays real-time status progress of the 802.1X authentication transaction.	Display only—Cannot configure.

CTL File Menu

The CTL File screen includes the options that are described in Table 4-20.

If a CTL file is installed on the phone, you can access the CTL File menu by pressing the **Settings** button and choosing **Security Configuration > CTL File**.

Table 4-20 CTL File Settings

Option	Description	To Change
CTL File	Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone. If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets. • A locked padlock icon in this option indicates that the CTL file is locked. • An unlocked padlock icon indicates that the CTL file is unlocked.	For more information about the CTL file, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified Communications Manager Security Guide*.
Unified CM/TFTP Server	IP address of a Cisco Unified Communications Manager and TFTP server used by the phone. Also displays a certificate icon if a certificate is installed for this server. If neither the primary TFTP (TFTP Server 1) server nor the backup TFTP server (TFTP Server 2) is listed in the CTL file, you must unlock the CTL file before you can save changes that you make to the TFTP Server 1 option or to the TFTP Server 2 option on the Network Configuration menu.	For information about changing these options, see the "Network Configuration Menu" section on page 4-5.
CAPF Server	IP address of the CAPF server used by the phone. Also displays a certificate icon if a certificate is installed for this server.	For more information about this server, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified Communications Manager Security Guide*.

Unlocking the CTL File

To unlock the CTL file from the Security Configuration menu, follow these steps:

Procedure

Step 1 Press **# to unlock options on the CTL File menu.

If you decide not to continue, press **# again to lock options on this menu.

Step 2 Highlight the CTL option.

Step 3 Press the **Unlock** softkey to unlock the CTL file.

After you change and save the applicable TFTP server option, the CTL file will be locked automatically.

Note When you press the **Unlock** softkey, it changes to **Lock**. If you decide not to change the TFTP server option, press the **Lock** softkey to lock the CTL file.

Trust List Menu

The Trust List menu displays information about all of the servers that the phone trusts and includes the options that are described in Table 4-21.

If a CTL file is installed on the phone, you can access the Trust List menu by pressing the **Settings** button and choosing **Security Configuration > Trust List**.

Table 4-21 Trust List Menu Settings

Option	Description	To Change
Unified CM/TFTP Server	IP address of a Cisco Unified Communications Manager and TFTP server used by the phone. Also displays a certificate icon if a certificate is installed for this server.	For more information about these settings, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified Communications Manager Security Guide*.
CAPF Server	IP address of the CAPF used by the phone. Also displays a certificate icon if a certificate is installed for this server.	For more information about these settings, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified Communications Manager Security Guide*.
SRST Router	IP address of the trusted SRST router that is available to the phone, if such a device has been configured in Cisco Unified Communications Manager Administration. Also displays a certificate icon if a certificate is installed for this server.	For more information about these settings, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified Communications Manager Security Guide*.

802.1X Authentication and Status

The 802.1X Authentication and 802.1X Authentication Status menus allow you to enable 802.1X authentication and monitor its progress. These options are described in Table 4-22 and Table 4-23.

You can access the 802.1X Authentication settings by pressing the **Settings** button and choosing **Security Configuration > 802.1X Authentication**. To exit this menu, press the **Exit** softkey.

Table 4-22 802.1X Authentication Settings

Option	Description	To Change
Device Authentication	Determines whether 802.1X authentication is enabled: • **Enabled**—Phone uses 802.1X authentication to request network access. • **Disabled**—Default setting in which the phone uses CDP to acquire VLAN and network access.	1. Choose **Settings > Security Configuration > 802.1X Authentication > Device Authentication**. 2. Set the Device Authentication option to Enabled or Disabled. 3. Press the **Save** softkey.
EAP-MD5	Specifies a password for use with 802.1X authentication using the following menu options (described in the following rows): • Device ID • Shared Secret • Realm	Choose **Settings > Security Configuration > 802.1X Authentication > EAP-MD5**.
	Device ID—Derivative of the phone's model number and unique MAC address displayed in this format: CP-<model>-SEP-<MAC>	Display only—Cannot configure.
	Shared Secret—Choose a password to use on the phone and on the authentication server. The password must be between 6 and 32 characters, consisting of any combination of numbers or letters. **Note** If you disable 802.1X authentication or perform a factory reset of the phone, the shared secret is deleted.	1. Choose **EAP-MD5 > Shared Secret**. 2. Enter the shared secret. 3. Press **Save**. See the "Troubleshooting Cisco Unified IP Phone Security" section on page 9-8 for assistance in recovering from a deleted shared secret.
	Realm—Indicates the user network domain, always set as *Network*	Display only—Cannot configure.

You can access the 802.1X Authentication Real-Time Status by pressing the **Settings** button and choosing **Security Configuration > 802.1X Authentication Status**. To exit this menu, press the **Exit** softkey.

Table 4-23 802.1X Authentication Real-Time Status

Option	Description	To Change
802.1X Authentication Status	Real-time progress of the 802.1X authentication status, displaying one of the following states: • Disabled—802.1X is disabled and transaction was not attempted • Disconnected—Physical link is down or disconnected • Connecting—Trying to discover or acquire the authenticator • Acquired—Authenticator acquired, awaiting authentication to begin • Authenticating—Authentication in progress • Authenticated—Authentication successful or implicit authentication due to timeouts • Held—Authentication failed, waiting before next attempt (approximately 60 seconds)	Display only—Cannot configure.

CHAPTER 5

Configuring Features, Templates, Services, and Users

After you install Cisco Unified IP Phones in your network, configure their network settings, and add them to Cisco Unified Communications Manager, you must use Cisco Unified Communications Manager Administration to configure telephony features, optionally modify phone templates, set up services, and assign users.

This chapter provides an overview of these configuration and setup procedures. Cisco Unified Communications Manager documentation provides detailed instructions for these procedures.

For suggestions about how to provide users with information about features, and what information to provide, see Appendix A, "Providing Information to Users Via a Website."

For information about setting up phones in non-English environments, see Appendix C, "Supporting International Users."

This chapter includes following topics:

- Telephony Features Available for the Phone, page 5-1
- Configuring Corporate and Personal Directories, page 5-16
- Modifying Phone Button Templates, page 5-17
- Configuring Softkey Templates, page 5-19
- Setting Up Services, page 5-20
- Adding Users to Cisco Unified Communications Manager, page 5-20
- Managing the User Options Web Pages, page 5-21

Telephony Features Available for the Phone

After you add Cisco Unified IP Phones to Cisco Unified Communications Manager, you can add functionality to the phones. Table 5-1 includes a list of supported telephony features, many of which you configure by using Cisco Unified Communications Manager Administration. The Configuration Reference column lists Cisco Unified Communications Manager documentation that contain configuration procedures and related information.

For information about using most of these features on the phone, refer to *Cisco Unified IP Phone 7970 Series Guide*. For a comprehensive listing of features on the phone, refer to *Cisco Unified IP Phone Features A–Z*.

Note Cisco Unified Communications Manager Administration also provides several service parameters that you can use to configure various telephony functions. For more information about service parameters and the functions that they control, refer to *Cisco Unified Communications Manager Administration Guide*.

Table 5-1 Telephony Features for the Cisco Unified IP Phone

Feature	Description	Configuration Reference
Abbreviated dialing	Allows users to speed dial a phone number by entering an assigned index code (1-99) on the phone keypad. Users assign index codes from the User Options web pages.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter.
Anonymous Call Block (SIP phones only)	Allows a user to reject calls from anonymous callers.	*Cisco Unified Communications Manager Administration Guide,* "SIP Profile Configuration" chapter.
Audible Message Waiting Indicator	A stutter tone from the handset, headset, or speakerphone indicates that a user has one or more new voice messages on a line. **Note** The stutter tone is line-specific. You hear it only when using the line with the waiting messages.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Message Waiting Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter.
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with either the speakerphone or the headset.	For more information, refer to *Cisco Unified Communications Manager Administration Guide,* "Configuring Directory Numbers" chapter.
Auto Dial	Allows the phone user to choose from matching numbers in the Placed Calls log while dialing. To place the call, the user can choose a number from the Auto Dial list or continue to enter digits manually.	
Auto-pickup	Allows a user to use one-touch pickup functionality for call pickup features.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Barge (and cBarge)	Allows a user to join a non-private call on a shared phone line. Barge features include cBarge and Barge. • cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features. • Barge adds a user to a call but does not convert the call into a conference. The phones support Barge in two conference modes: • Built-in conference bridge at the target device (the phone that is being barged). This mode uses the **Barge** softkey. • Shared conference bridge. This mode uses the **cBarge** softkey.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Barge and Privacy" chapter.
Block external to external transfer	Prevents users from transferring an external call to another external number.	For more information, refer to *Cisco Unified Communications Manager Features and Services Guide*, "External Call Transfer Restrictions" chapter.
Busy Lamp Field (BLF)	Allows a user to monitor the call state of a directory number associated with a speed-dial button, call log, or directory listing on the phone.	For more information, refer to *Cisco Unified Communications Manager Features and Services Guide*, "Presence" chapter.
Busy Lamp Field (BLF) pickup	Provides enhancements to BLF speed dial. Allows you to configure a directory number (DN) that a user can monitor for incoming calls. When the DN receives an incoming call, the system alerts the monitoring user, who can then pick up the call.	For more information, refer to *Cisco Unified Communications Manager Feature and Services Guide,* "Call Pickup" chapter.
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.	For more information, refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Call Back" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Call display restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Understanding Route Plans" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Call Display Restrictions" chapter.
Call forward	Allows users to redirect incoming calls to another number. Call forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Directory Number Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter. • Specifying Options that Appear on the User Options Web Pages, page 5-21
Call forward all destination override	Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the CFA initiator. This feature allows the CFA target to reach the CFA initiator for important calls. The override works whether the CFA target phone number is internal or external.	For more information, refer to *"Cisco Unified Communications Manager System Guide,* "Understanding Directory Numbers" chapter.
Call forward all loop breakout	Detects and prevents Call Forward All loops. When a Call Forward All loop is detected, the Call Forward All configuration is ignored and the call rings through.	For more information, refer to the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Call forward all loop prevention	Prevents a user from configuring a Call Forward All destination directly on the phone that creates a Call Forward All loop or that creates a Call Forward All chain with more hops than the existing *Forward Maximum Hop Count* service parameter allows.	For more information, refer to the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Call forward configurable display	Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide*. • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Call park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager system.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Call Park" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Call Park" chapter.
Call pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone. You can configure an audio and/or visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.
Call recording	Allows a supervisor to record an active call. The user might hear an intermittent tone (beep tone) during a call when it is being recorded. **Note** The intercom feature is disabled when a call is being monitored or recorded.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide,* "Monitoring and Recording" chapter.
Call waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Displays incoming call information on the phone screen.	For more information, refer to the *Cisco Unified Communications System Guide*, "Understanding Directory Numbers" chapter.
Caller ID	Displays caller identification such as a phone number, name, or other descriptive text on the phone screen.	For more information, refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter." • *Cisco Unified Communications Manager System Guide,* "Understanding Route Plans" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Call Display Restrictions" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Caller ID Blocking	Allows users to block their phone numbers or e-mail addresses from displaying on phones that have caller identification enabled.	For more information, refer to: • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" chapter. • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter. • *Cisco Unified Communications Manager Administration Guide*, "SIP Profile Configuration" chapter.
Cisco Unified Communications Manager Assistant	Enables managers and their assistants to work together more effectively by providing a call-routing service, enhancements to phone capabilities for the manager, and desktop interfaces that are primarily used by the assistant.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified CM Assistant Configuration Wizard" chapter. • *Cisco Unified Communications Manager System Guide, "*Cisco Unified Communications Manager Assistant" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Communications Manager Assistant With Proxy Line Support" and "Cisco Unified Communications Manager Assistant With Shared Line Support" chapters.
Client matter codes (CMC) (SCCP phones only)	Enables a user to specify that a call relates to a specific client matter.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide, "*Client Matter Codes" chapter. • *Cisco Unified Communications Manager Features and Services Guide, "*Client Matter Codes and Forced Authorization Codes" chapter.
Computer Telephony Integration (CTI) applications	A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection.	For more information, refer to the *Cisco Unified Communications Manager Administration Guide, "*CTI Route Point Configuration" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Conference	• Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference, Join, cBarge, and Meet-Me. • Allows a non-initiator in a standard (ad hoc) conference to add or remove participants; also allows any conference participant to join together two standard conferences on the same line.	• For more information, refer to *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter. • The service parameter, Advance Adhoc Conference, (disabled by default in Cisco Unified Communications Manager Administration) allows you to enable these features. **Note** Be sure to inform your users whether these features are activated.
Configurable call forward display	Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide, "*Directory Number Configuration" chapter. • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Directed Call Park	Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. A Call Park BLF button indicates whether a directed call park number is occupied and provides speed-dial access to the directed call park number. **Note** If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features.	For more information refer to *Cisco Unified Communications Manager Features and Services Guide, "*Call Park and Directed Call Park" chapter.
Direct transfer (SCCP phones only)	Allows users to connect two calls to each other (without remaining on the line).	For more information, refer to *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Directed call pickup	Allows a user to answer a call that is ringing on a particular directory number.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.
Distinctive ring	Users can customize how their phone indicates an incoming call and a new voice mail message.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Custom Phone Rings" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Do Not Disturb (DND)	When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur. You can configure the phone to have a softkey template with a DND softkey or a phone-button template with DND as one of the selected features. The following DND-related parameters are configurable in Cisco Unified Communications Manager Administration: • Do Not Disturb—Choose **Device > Phone > Phone Configuration**. • DND Option—Choose "Call Reject" (to turn off all audible and visual notifications), or "Ringer Off" (to turn off only the ringer). *DND Option* appears on both the Common Phone Profile window and the Phone Configuration window (Phone Configuration window value takes precedence). • DND Incoming Call Alert—Choose the type of alert to play, if any, on a phone for incoming calls when DND is active. This parameter is located on both the Common Phone Profile window and the Phone Configuration window (Phone Configuration window value takes precedence). • BLF Status Depicts DND—Enables DND status to override busy/idle state.	*Cisco Unified Communications Manager Features and Services Guide*, "Do Not Disturb" chapter.
Extension Mobility Service	Allows a user to temporarily apply a phone number and user profile settings to a shared Cisco Unified IP Phone by logging into the Extension Mobility service on that phone. Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers.	For more information, refer to: • *Cisco Unified Communications Manager Features and Services Guide,* "Cisco Unified Communications Manager Extension Mobility" chapter. • *Cisco Unified Communications Manager System Guide*, "Cisco Unified Communications Manager Extension Mobility and Phone Login Features" chapter.
Fast Dial Service	Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries. (See "Services" in this table.)	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Services Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone Services" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Forced authorization codes (FAC) (SCCP phones only)	Controls the types of calls that certain users can place.	For more information, refer to: • *Cisco Unified Communications Manager System Guide*, "Forced Authorization Codes (FAC)" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Client Matter Codes and Forced Authorization Codes" chapter.
Group call pickup	Allows a user to answer a call that is ringing on a directory number in another group.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.
Help system	Provides a comprehensive set of topics that appear on the phone screen.	Requires no configuration.
Hold/Resume	Allows the user to move a connected call between an active state and a held state.	• Requires no configuration, unless you want to use music on hold. See "Music on Hold" in this table for information. • See also: "Hold Reversion" in this table.
Hold Reversion	Limits the amount of time that a call can be on hold before reverting back to the phone that put the call on hold and alerting the user. Reverting calls are distinguished from incoming calls by a single ring (or beep, depending on the new call indicator setting for the line). This notification repeats at intervals if not resumed. A call that triggers Hold Reversion also displays an animated icon in the call bubble and a brief message on the status line. You can configure call focus priority to favor incoming or reverting calls.	For more information about configuring this feature, refer to *Cisco Unified Communications Manager Features and Services Guide,* "Hold Reversion" chapter.
Hunt Group	Provides load sharing for calls to a main directory number. A hunt group contains a series of directory numbers that can answer the incoming calls. When the first directory number in the hunt group is busy, the system hunts in a predetermined sequence for the next available directory number in the group and directs the call to that phone.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Hunt Group Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Understanding Route Plans" chapter.
Immediate Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system.When a call is diverted, the line becomes available to make or receive new calls.	For more information, refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Immediate Divert" chapter

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Immediate Divert—Enhanced	Allows users to transfer incoming calls directly to their voice messaging system or to the voice messaging system of the original called party.	For more information, refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Call Park and Directed Call Park" chapter
Intercom	Allows users to place and receive intercom calls using programmable phone buttons. You can configure intercom line buttons to: • Directly dial a specific intercom extension. • Initiate an intercom call and then prompt the user to enter a valid intercom number. **Note** If your user logs into the same phone on a daily basis using their Cisco Extension Mobility profile, assign the phone button template that contains intercom information to their profile, and assign the phone as the default intercom device for the intercom line.	• *Cisco Unified CallManager Feature and Services Guide*, Release 7.0, "Intercom chapter" • *Cisco Unified CallManager Feature and Services Guide*, Release 7.0, "Cisco Extension Mobility" chapter"
Join/Select	Creates a conference by joining together existing calls that are on a single phone line.	For more information, refer to the *Cisco Unified IP Phone Guide*, "Basic Call Handling" chapter, "Making Conference Calls" section.
Join Across Lines/Select	Allows users to apply the Join feature to calls that are on multiple phone lines.	For more information: • See Configuring Softkey Templates, page 5-19. • Refer to *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Log out of hunt groups	Allows users to log out of a hunt group and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent non-hunt group calls from ringing their phone.	For more information • See Configuring Softkey Templates, page 5-19. • *Cisco Unified Communications Manager System Guide,* "Understanding Route Plans" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Malicious call identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received.	For more information refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Malicious Call Identification" chapter.
Meet-Me conference	Allows a user to host a Meet-Me conference in which other participants call a predetermined number at a scheduled time.	For more information refer to *Cisco Unified Communications Manager Administration Guide*, "Meet-Me Number/Pattern Configuration" chapter.
Message waiting indicator	A light on the handset that indicates that a user has one or more new voice messages.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Message Waiting Configuration" chapter. • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter.
Mobile Connect	Enables users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and a remote device such as a mobile phone. Users can restrict the group of callers according to phone number and time of day.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Mobile Connect and Mobile Voice Access" chapter.
Mobile Voice Access	Extends Mobile Connect capabilities by allowing users to access an interactive voice response (IVR) system to originate a call from a remote device such as a mobile phone.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Mobile Connect and Mobile Voice Access" chapter.
Multilevel Precedence and Preemption (MLPP) (SCCP phones only)	Provides a method of prioritizing calls within your phone system. Use this feature when users work in an environment where they need to make and receive urgent or critical calls.	For more information refer to *Cisco Unified Communications Manager Features and Services Guide,* "Multilevel Precedence and Preemption" chapter.
Multiple calls per line appearance	Each line can support multiple calls. Only one call can be active at any time; other calls are automatically placed on hold.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Music on hold	Plays music while callers are on hold.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide*, "Music On Hold Audio Source Configuration" and "Music On Hold Server Configuration" chapters. • *Cisco Unified Communications Manager System Guide*, "Music on Hold" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Music On Hold" chapter.
Mute	Mutes the microphone from the handset or headset.	Requires no configuration.
Onhook call transfer	Allows a user to press a single Transfer softkey and then go onhook to complete a call transfer.	For more information refer to *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter.
Onhook predialing	Allows a user to dial a number without going off hook. The user can then either pick up the handset or press the Dial softkey.	For more information, refer to the *Cisco Unified IP Phone Guide*, "Basic Call Handling" chapter.
Other group pickup	Allows a user to answer a call ringing on a phone in another group that is associated with the user's group.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.
Presence-enabled directories	Allows a user to monitor the call state of another directory number (DN) listed in call logs, speed dials, and corporate directories. The Busy Lamp Field (BLF) for the DN displays the call state.	For more information, refer to *Cisco Unified Communications Manager Features and Services Guide*, "Presence" chapter.
Private Line Automated Ringdown (PLAR)	The Cisco Unified Communications Manager administrator can configure a phone number that the Cisco Unified IP Phone dials as soon as the handset goes off hook. This can be useful for phones that are designated for calling emergency or "hotline" numbers.	Refer to *Cisco Unified Communications Manager System Guide, "*SIP Dial Rules Configuration" chapter.
Privacy	Prevents users who share a line from adding themselves to a call and from viewing information on their phone screens about the call of the other user.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide, "*Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide* "Barge and Privacy" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Programmable line keys	The administrator can assign features to line buttons. Softkeys normally control these features; for example, New Call, Call Back, End Call, and Forward All. When the administrator configures these features on the line buttons, they always remain visible, so users can have a "hard" New Call key.	For more information, refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter • *Cisco Unified Communications Manager Administration Guide*, "Modifying Phone Button Templates"
Protected calling	Provides a secure (encrypted) connection between two phones. A security tone is played at the beginning of the call to indicate that both phones are protected. Some features, such as conference calling, shared lines, Extension Mobility, and Join Across Lines are not available when protected calling is configured. Protected calls are not authenticated.	For more information about security, see the "Overview of Supported Security Features" section on page 1-10. For additional information, refer to *Cisco Unified Communications Manager Security Guide.*
Quality Reporting Tool (QRT)	Allows users to use the QRT softkey on a phone to submit information about problem phone calls. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.	For more information refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Quality Report Tool" chapter.
Redial	Allows users to call the most recently dialed phone number by pressing a softkey.	Requires no configuration.
Ring setting	Identifies ring type used for a line when a phone has another active call.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter. • "Creating Custom Phone Rings" section on page 6-2.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Secure Conference	• Allows secure phones to place conference calls by using a secured conference bridge. • As new participants are added by using Confrn, Join, cBarge, Barge softkeys or MeetMe conferencing, the secure call icon displays as long as all participants use secure phones. • The Conference List displays the security level of each conference participant. Initiators can remove non-secure participants from the Conference List. (Non-initiators can add or remove conference participants if the AdvanceAdhocConference parameter is set.)	For more information about security, see the "Overview of Supported Security Features" section on page 1-10. For additional information, refer to these: • *Cisco Unified Communications Manager System Guide*, "Conference Bridges" chapter • *Cisco Unified Communications Manager Administration Guide,* "Conference Bridge Configuration" chapter • *Cisco Unified Communications Manager Security Guide.*
Services	Allows you to use the Cisco Unified IP Phone Services Configuration menu in Cisco Unified Communications Manager Administration to define and maintain the list of phone services to which users can subscribe.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone Services" chapter.
Services URL button	Allows users to access services from a programmable button rather than by using the Services menu on a phone.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone Services" chapter.
Shared line	Allows a user to have several phones that share the same phone number or allows a user to share a phone number with a coworker.	For more information refer to *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter.
Silent Monitoring	Allows a supervisor to silently monitor an active call. The supervisor cannot be heard by either party on the call. The user might hear an intermittent tone (beep tone) during a call when it is being monitored. **Note** The intercom feature is disabled when a call is being monitored or recorded.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide,* "Monitoring and Recording" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Single Button Barge	Allows users to press a line key to Barge or cBarge into a remote-in-use call on a shared line.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide*, "Device Pool Configuration" chapter. • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Barge and Privacy" chapter.
Speed dialing	Dials a specified number that has been previously stored.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phones" chapter.
Time-of-Day Routing	Restricts access to specified telephony features by time period.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Time Period Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Time-of-Day Routing" chapter.
Touchscreen illumination disabling	Allows user to disable touchscreen illumination on a phone, which would override other rules that determine when the touchscreen gets illuminated. To provide this feature, you must implement the Display URI, which includes configuring the length of time that illumination remains disabled.	Refer to the *Cisco Unified IP Phone Service Application Development Notes* at the following location: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html
Transfer-direct transfer	Transfer—The first invocation of Transfer will always initiate a new call by using the same directory number, after putting the active call on hold. Direct Transfer—This transfer joins two established calls (call is in hold or in connected state) into one call and drops the feature initiator from the call. Direct Transfer does not initiate a consultation call and does not put the active call on hold.	For more information, refer to the *Cisco Unified Communications Manager Administration Guide,* "Understanding Directory Numbers" chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Video mode (SCCP phones only)	Allows a user to select the video display mode for viewing a video conference, depending on the modes configured in the system.	For more information: • Refer to *Cisco Unified Communications Manager Administration Guide,* "Conference Bridge Configuration" chapter. • Refer to *Cisco Unified Communications Manager System Guide,* "Understanding Video Telephony" chapter.
Video support (SCCP phones only)	Enable video support on the phone.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Conference Bridge Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Understanding Video Telephony" chapter. • *Cisco VT Advantage Administration Guide*, "Overview of Cisco VT Advantage" chapter.
Voice-messaging system	Enables callers to leave messages if calls are unanswered.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Voice-Mail Port Configuration" chapter. • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter.

Configuring Corporate and Personal Directories

The **Directories** button on the Cisco Unified IP Phone 7970 Series gives users access to several directories. These directories can include:

- Corporate Directory—Allows a user to look up phone numbers for co-workers.

  To support this feature, you must configure corporate directories. See the "Configuring Corporate Directories" section on page 5-17 for more information.

- Personal Directory—Allows a user to store a set of personal numbers.

  To support this feature, you must provide the user with software to configure the personal directory. See the "Configuring Personal Directory" section on page 5-17 for more information.

Configuring Corporate Directories

Cisco Unified Communications Manager uses a Lightweight Directory Access Protocol (LDAP) directory to store authentication and authorization information about users of Cisco Unified Communications Manager applications that interface with Cisco Unified Communications Manager. Authentication establishes a user's right to access the system. Authorization identifies the telephony resources that a user is permitted to use, such as a specific telephone extension.

To install and set up these features, refer to the *Cisco Unified Communications Manager Administration Guide*, LDAP System Configuration, LDAP Directory Configuration, and LDAP Authentication Configuration chapters.

Configuring Personal Directory

Personal Directory consists of the following features:

- Personal Address Book (PAB)
- Personal Fast Dials (Fast Dials)
- Address Book Synchronization Tool (TABSynch)

Users can access Personal Directory features by these methods:

- From a web browser—Users can access the PAB and Fast Dials features from the Cisco Unified Communications Manager User Options web pages
- From the Cisco Unified IP Phone—Users can choose **Directories > Personal Directory** to access the PAB and Fast Dials features from their phones

From a Microsoft Windows application—Users can use the TABSynch tool to synchronize their PABs with Microsoft Windows Address Book (WAB). Customers who want to use the Microsoft Outlook Address Book (OAB) should begin by importing the data from the OAB into the Windows Address Book (WAB). TabSync can then be used to synchronize the WAB with Personal Directory.

To configure Personal Directory from a web browser, users must access their User Options web pages. You must provide users with a URL and login information.

To synchronize with Microsoft Outlook, users must install the TABSynch utility, which is provided by you. To obtain the TABSynch software to distribute to users, choose **Application > Plugins** from Cisco Unified Communications Manager Administration, then locate and click **Cisco Unified IP Phone Address Book Synchronizer**.

Modifying Phone Button Templates

Phone button templates let you assign speed dials and call-handling features to programmable line buttons. Call-handling features that can be assigned to buttons include call forward, hold, and conference.

Ideally, you modify templates before registering phones on the network. In this way, you can access customized phone button template options from Cisco Unified Communications Manager during registration.

To modify a phone button template, choose **Device > Device Settings > Phone Button Template** from Cisco Unified Communications Manager Administration. To assign a phone button template to a phone, use the Phone Button Template field in the Cisco Unified Communications Manager Administration Phone configuration window. Refer to *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* for more information.

The default Cisco Unified IP Phone 7970 Series template that ships with the phone uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dial.

The recommended standard Cisco Unified IP Phone 7970 Series template uses buttons 1 and 2 for lines, assigns buttons 3 through 5 as speed dial, and buttons 6 through 8 as Hold, Conference, and Transfer, respectively.

To avoid confusion for users, do not assign a feature to a button and a softkey at the same time.

For more information about softkey templates, see Configuring Softkey Templates, page 5-19.

Modifying a Phone Button Template for Personal Address Book or Fast Dials

You can modify a phone button template to associate a service URL with a line button. Doing so enables users to have single-button access to the PAB and Fast Dials. Before you modify the phone button template, you must configure PAB or Fast Dials as an IP phone service.

To configure PAB or Fast Dial as an IP phone service (if it is not already a service), follow these steps:

Procedure

Step 1 Choose **Device >Device Settings > Phone Services**.

The Find and List IP Phone Services window displays.

Step 2 Click **Add New**. The IP phone services Configuration window displays.

Step 3 Enter the following settings:

- Service Name and ASCII Service Name—Enter **Personal Address Book**.
- Service Description—Enter an optional description of the service.
- Service URL

  For PAB, enter the following URL:

  http://<*Unified CM-server-name*>:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab

  For Fast Dial, enter the following URL:

  http://<*Unified-CM-server-name*>:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd
- Service Category—Select **XML Service**.
- Service Type—Select **Directories**.
- Enable—Select the check box.

Step 4 Click **Save**.

You can add, update, or delete service parameters as needed as described in "IP Phone Service Parameter" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Note If you change the service URL, remove an IP phone service parameter, or change the name of a phone service parameter for a phone service to which users are subscribed, you must click **Update Subscriptions** to update all currently subscribed users with the changes, or users must resubscribe to the service to rebuild the correct URL.

To modify a phone button template for PAB or Fast Dial, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Phone Button Template**.

Step 2 Click **Find**.

Step 3 Select the phone model.

Step 4 Click **Copy**, enter a name for the new template, and then click **Save**.

The Phone Button Template Configuration window opens.

Step 5 Identify the button you would like to assign, and select **Service URL** from the Features drop-down list box associated with the line.

Step 6 Click **Save** to create a new phone button template using the service URL.

Step 7 Choose **Device > Phone** and open the Phone Configuration window for the phone.

Step 8 Select the new phone button template from the Phone Button Template drop-down list box.

Step 9 Click **Save** to store the change and then click **Reset** to implement the change.

The phone user can now access the User Options pages and associate the service with a button on the phone.

For additional information on IP phone services, see the *Cisco Unified Communications Manager Administration Guide,* "IP Phone Services Configuration" chapter. For additional information on configuring line buttons, see the *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter, "Configuring Speed-Dial Buttons" section.

Configuring Softkey Templates

Using Cisco Unified Communications Manager Administration, you can manage softkeys associated with applications that are supported by the Cisco Unified IP Phone 7970 Series.
Cisco Unified Communications Manager supports two types of softkey templates: standard and nonstandard. Standard softkey templates include Standard User, Standard Feature, Standard Assistant, Standard Manager, and Standard Shared Mode Manager An application that supports softkeys can have one or more standard softkey templates associated with it. You can modify a standard softkey template by making a copy of it, giving it a new name, and making updates to that copied softkey template. You can also modify a nonstandard softkey template.

To configure softkey templates, choose **Device > Device Settings > Softkey Template** from Cisco Unified Communications Manager Administration. To assign a softkey template to a phone, use the Softkey Template field in the Cisco Unified Communications Manager Administration Phone configuration window. Refer to *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* for more information.

Setting Up Services

The **Services** button on the Cisco Unified IP Phone gives users access to Cisco Unified IP Phone Services. You can also assign services to the programmable buttons on the phone (refer to *Cisco Unified IP Phone 7970 Series Guide* for more information). These services comprise XML applications that enable the display of interactive content with text and graphics on the phone. Examples of services include local movie times, stock quotes, and weather reports.

Before a user can access any service:

- You must use Cisco Unified Communications Manager Administration to configure available services.
- The user must subscribe to services by using the Cisco Unified IP Phone User Options web pages. This web-based application provides a graphical user interface (GUI) for limited, end-user configuration of IP Phone applications.

Before you set up services, gather the URLs for the sites that you want to set up and verify that users can access those sites from your corporate IP telephony network.

To set up these services, choose **Device > Device Settings > Phone Services** from Cisco Unified Communications Manager Administration. Refer to *Cisco Unified Communications Manager Administration Guide* and to *Cisco Unified Communications Manager System Guide* for more information.

After you configure these services, verify that your users have access to the Cisco Unified Communications Manager IP Phone Options web-based application, from which they can select and subscribe to configured services. See the "How Users Subscribe to Services and Configure Phone Features" section on page A-3 for a summary of the information that you must provide to end users.

Adding Users to Cisco Unified Communications Manager

Adding users to Cisco Unified Communications Manager allows you to display and maintain information about users and allows each user to perform these tasks:

- Access the corporate directory and other customized directories from a Cisco Unified IP Phone
- Create a personal directory
- Set up speed dial and call forwarding numbers
- Subscribe to services that are accessible from a Cisco Unified IP Phone

You can add users to Cisco Unified Communications Manager using either of these methods:

- To add users individually, choose **User Management > End User** from Cisco Unified Communications Manager Administration.

Refer to *Cisco Unified Communications Manager Administration Guide* for more information about adding users. Refer to *Cisco Unified Communications Manager System Guide* for details about user information.

- To add users in batches, use the Bulk Administration Tool. This method also enables you to set an identical default password for all users.

  Refer to *Cisco Unified Communications Manager Bulk Administration Guide* for details.

Managing the User Options Web Pages

From the User Options web page, users can customize and control several phone features and settings. For detailed information about the User Options web pages, refer to *Cisco Unified IP Phone 7970 Series Phone Guide*.

Giving Users Access to the User Options Web Pages

Before a user can access the User Options web pages, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager end user group. To do so, choose **User Management > User Group**. You must also associate appropriate phones with the user. To perform these procedures, from Cisco Unified Communications Manager Administration, choose **User Management > End User**.

For additional information, refer to *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" section.

Specifying Options that Appear on the User Options Web Pages

Most options that are on the User Options web pages appear by default. However, the following options must be set by the system administrator by using Enterprise Parameters Configuration settings in Cisco Unified Communications Manager Administration:

- Show Ring Settings
- Show Line Text Label Settings
- Show Call Forwarding

Note The settings apply to all User Options web pages at your site.

To specify the options that appear on the User Options web pages, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters.**

The Enterprise Parameters Configuration window displays.

Step 2 In the CCMUser Parameters area, specify whether a parameter appears on the User Options web pages by choosing one of these values from the **Parameter Value** drop-down list box for the parameter:

- **True**—Option displays on the User Options web pages (default).
- **False**—Option does not display on the User Options web pages.
- **Show All Settings**—All call forward settings display on the User Options web pages (default).
- **Hide All Settings**—No call forward settings display on the User Options web pages.
- **Show Only Call Forward All**—Only call forward all calls displays on the User Options web pages.

CHAPTER 6

Customizing the Cisco Unified IP Phone

This chapter explains how you customize configuration files, phone ring sounds, background images, and other phone features.

This chapter includes these topics:

- Customizing and Modifying Configuration Files, page 6-1
- Creating Custom Phone Rings, page 6-2
- Creating Custom Background Images, page 6-3
- Configuring Wideband Codec, page 6-6
- Configuring the Idle Display, page 6-7
- Automatically Disabling the Cisco Unified IP Phone Touchscreen, page 6-7

Customizing and Modifying Configuration Files

You can modify configuration files (for example, edit the xml files) and add customized files (for example, custom ring tones, call back tones, phone backgrounds) to the TFTP directory. You can modify files and add customized files to the TFTP directory in Cisco Unified Communications Operating System Administration, from the TFTP Server File Upload window. Refer to *Cisco Unified IP Telephony Platform Administration Guide* for information about how to upload files to the TFTP folder on a Cisco Unified Communications Manager server.

You can obtain a copy of the Ringlist.xml and List.xml files from the system by using the following admin command-line interface (CLI) “file” commands:

- admin:file
  - file list*
  - file view*
  - file search*
  - file get*
  - file dump*
  - file tail*
  - file delete*

Creating Custom Phone Rings

The Cisco Unified IP Phone ships with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco Unified Communications Manager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named Ringlist.xml) that describes the ring list options that are available at your site, exist in the TFTP directory on each Cisco Unified Communications Manager server.

For more information, see the "Cisco TFTP" chapter in *Cisco Unified Communications Manager System Guide* and the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide.*

The following sections describe how you can customize the phone rings that are available at your site by creating PCM files and editing the Ringlist.xml file:

- Ringlist.xml File Format Requirements, page 6-2
- PCM File Requirements for Custom Ring Types, page 6-3
- Configuring a Custom Phone Ring, page 6-3

Ringlist.xml File Format Requirements

The Ringlist.xml file defines an XML object that contains a list of phone ring types. This file can include up to 50 ring types. Each ring type contains a pointer to the PCM file that is used for that ring type and the text that will appear on the Ring Type menu on a Cisco Unified IP Phone for that ring. The Cisco TFTP server for each Cisco Unified Communications Manager contains this file.

The CiscoIPPhoneRinglist XML object uses the following simple tag set to describe the information:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRingList>
```

The following characteristics apply to the definition names. You must include the required DisplayName and FileName for each phone ring type.

- DisplayName defines the name of the custom ring for the associated PCM file that will display on the Ring Type menu of the Cisco Unified IP Phone.
- FileName specifies the name of the PCM file for the custom ring to associate with DisplayName.

Note The DisplayName and FileName fields must not exceed 25 characters.

This example shows a Ringlist.xml file that defines two phone ring types:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.raw</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.raw</FileName>
   </Ring>
</CiscoIPPhoneRingList>
```

PCM File Requirements for Custom Ring Types

The PCM files for the rings must meet the following requirements for proper playback on Cisco Unified IP Phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- uLaw compression
- Maximum ring size—16080 samples
- Minimum ring size—240 samples
- Number of samples in the ring is evenly divisible by 240.
- Ring starts and ends at the zero crossing.
- To create PCM files for custom phone rings, you can use any standard audio editing packages that supports these file format requirements.

Configuring a Custom Phone Ring

To create custom phone rings for the Cisco Unified IP Phone 7970 Series, follow these steps:

Procedure

Step 1 Create a PCM file for each custom ring (one ring per file). Ensure the PCM files comply with the format guidelines that are listed in the "PCM File Requirements for Custom Ring Types" section on page 6-3.

Step 2 Place the new PCM files that you created to the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster. For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide.*

Step 3 Use a text editor to edit the Ringlist.xml file. See the "Ringlist.xml File Format Requirements" section on page 6-2 for information about how to format this file and for a sample Ringlist.xml file.

Step 4 Save your modifications and close the Ringlist.xml file.

Step 5 To cache the new Ringlist.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and re-enable the Enable Caching of Constant and Bin Files at Startup TFTP service parameter (located in the Advanced Service Parameters).

Creating Custom Background Images

You can provide users with a choice of background images for the LCD screen on their phones. Users can select a background image by choosing **Settings > User Preferences > Background Images** on the phone.

The image choices that users see come from PNG images and an XML file (called List.xml) that are stored on the TFTP server used by the phone. By storing your own PNG files and editing the XML file on the TFTP server, you can designate the background images from which users can choose. In this way, you can provide custom images, such as your company logo.

The following sections describe how you can customize the background images that are available at your site by creating your own PNG files and editing the List.xml file:

- List.xml File Format Requirements, page 6-4.
- PNG File Requirements for Custom Background Images, page 6-5.
- Configuring a Custom Background Image, page 6-5

List.xml File Format Requirements

The List.xml file defines an XML object that contains a list of background images. The List.xml file is stored in the following subdirectory on the TFTP server:

/Desktops/320x212x12

Tip If you are manually creating the directory structure and the List.xml file, you must ensure that the directories and files can be accessed by the user\CCMService, which is used by the TFTP service.

For more information, see the "Cisco TFTP" chapter in *Cisco Unified Communications Manager System Guide* and the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide.*

The List.xml file can include up to 50 background images. The images are in the order that they appear in the Background Images menu on the phone. For each image, the List.xml file contains one element type, called ImageItem. The ImageItem element includes these two attributes:

- Image—Uniform resource identifier (URI) that specifies where the phone obtains the thumbnail image that will appear on the Background Images menu on a Phone.
- URL—URI that specifies where the phone obtains the full size image.

The following example shows a List.xml file that defines two images. The required Image and URL attributes must be included for each image. The TFTP URI that is shown in the example is the only supported method for linking to full size and thumbnail images. HTTP URL support is not provided.

List.xml Example

```
<CiscoIPPhoneImageList>
<ImageItem Image="TFTP:Desktops/320x212x12/TN-Fountain.png"
URL="TFTP:Desktops/320x212x12/Fountain.png"/>
<ImageItem Image="TFTP:Desktops/320x212x12/TN-FullMoon.png"
URL="TFTP:Desktops/320x212x12/FullMoon.png"/>
</CiscoIPPhoneImageList>
```

The Cisco Unified IP Phone firmware includes a default background image. This image is not defined in the List.xml file. The default image is always the first image that appears in the Background Images menu on the phone.

PNG File Requirements for Custom Background Images

Each background image requires two PNG files:

- Full size image—Version that displays on the on the phone.
- Thumbnail image—Version that displays on the Background Images screen from which users can select an image. Must be 25% of the size of the full size image.

Tip Many graphics programs provide a feature that will resize a graphic. An easy way to create a thumbnail image is to first create and save the full size image, then use the sizing feature in the graphics program to create a version of that image that is 25% of the original size. Save the thumbnail version by using a different name.

The PNG files for background images must meet the following requirements for proper display on the Cisco Unified IP Phone:

- Full size image—320 pixels (width) X 212 pixels (height).
- Thumbnail image—80 pixels (width) X 53 pixels (height).
- Color palette (applies to Cisco Unified IP Phone 7970 Series only)—Includes up to 12-bit color (4096 colors). You can use more than 12-bit color, but the phone will reduce the color palette to12-bit before displaying the image. For best results, reduce the color palette of an image to 12-bit when you create a PNG file.

Tip If you are using a graphics program that supports a posterize feature for specifying the number of tonal levels per color channel, set the number of tonal levels per channel to 16 (16 red X 16 green X 16 blue = 4096 colors).

Configuring a Custom Background Image

To create custom background images for the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1 Create two PNG files for each image (a full size version and a thumbnail version). Ensure the PNG files comply with the format guidelines that are listed in the "PNG File Requirements for Custom Background Images" section on page 6-5.

Step 2 Upload the new PNG files that you created to the following subdirectory in the TFTP server for the Cisco Unified Communications Manager:

/Desktops/320x212x12

Note The file name and subdirectory parameters are case sensitive. Be sure to use the forward slash "/" when you specify the subdirectory path.

To upload the files, choose **Software Upgrades > Upload TFTP Server File** in Cisco Unified Communications Operating System Administration. For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

Note If the folder does not exist, the folder is created and the files are uploaded to the folder.

Step 3 You must also copy the customized images and files to the other TFTP servers that the phone may contact to obtain these files.

Note Cisco recommends that you also store backup copies of custom image files in another location. You can use these backup copies if the customized files are overwritten when you upgrade Cisco Unified Communications Manager.

Step 4 Use a text editor to edit the List.xml file. See the "List.xml File Format Requirements" section on page 6-4 for the location of this file, formatting requirements, and a sample file.

Step 5 Save your modifications and close the List.xml file.

Note When you upgrade Cisco Unified Communications Manager, a default List.xml file will replace your customized List.xml file. After you customize the List.xml file, make a copy of the file and store it in another location. After upgrading Cisco Unified Communications Manager, replace the default List.xml file with your stored copy.

Step 6 To cache the new List.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and reenable the Enable Caching of Constant and Bin Files at Startup TFTP service parameter (located in the Advanced Service Parameters).

Configuring Wideband Codec

If Cisco Unified Communications Manager has been configured to use G.722 (G.722 is enabled by default for the Cisco Unified IP Phone 7970 Series) and if the far endpoint supports G.722, the call connects using the G.722 codec in place of G.711. This situation occurs regardless of whether the user has enabled a wideband headset or wideband handset, but if either the headset or handset is enabled, the user may notice greater audio sensitivity during the call. Greater sensitivity means improved audio clarity but also means that more background noise can be heard by the far endpoint—noise such as rustling papers or nearby conversations. Even without a wideband headset or handset, some users may prefer the additional sensitivity of G.722. Other users may be distracted by the additional sensitivity of G.722.

The following parameters in Cisco Unified Communications Manager Administration affect whether wideband is supported for this Cisco Unified Communications Manager server or a specific phone:

- Advertise G.722 Codec—From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**. The default value of this enterprise parameter is True, which means that all Cisco Unified IP Phone Series that are registered to this Cisco Unified Communications Manager advertise G.722 to Cisco Unified Communications Manager. If each endpoint in the attempted call supports G.722 in its capabilities set, Cisco Unified Communications Manager chooses that codec for the call.

- Advertise G.722 Codec—From Cisco Unified Communications Manager Administration, choose **Device > Phone**. The default value for this product-specific parameter is the value that is specified in the enterprise parameter. If you want to override this on a per-phone basis, choose Enabled or Disabled in the Advertise G.722 Codec parameter on the Product Specific Configuration area of the Phone Configuration window.

Configuring the Idle Display

You can specify an idle display that appears on the phone LCD screen. The idle display is an XML service that the phone invokes when the phone has been idle (not in use) for a designated period and no feature menu is open.

XML services that can be used as idle displays include company logos, product pictures, and stock quotes.

Configuring the idle display consists of these general steps.

1. Formatting an image for display on the phone.
2. Configure Cisco Unified Communications Manager to display the image on the phone.

For detailed instructions about creating and displaying the idle display, refer to *Creating Idle URL Graphics on Cisco Unified IP Phone* at this URL:

http://www.cisco.com/warp/public/788/AVVID/idle-url.html

In addition, you can refer to *Cisco Unified Communications Manager Administration Guide* or to *Cisco Unified Communications Manager Bulk Administration Guide* for the following information:

- Specifying the URL of the idle display XML service:
  - For a single phone—Idle field on the Cisco Unified Communications Manager Phone configuration window
  - For multiple phones simultaneously—URL Idle field on the Cisco Unified Communications Manager Enterprise Parameters configuration window, or the Idle field in the Bulk Administration Tool (BAT)
- Specifying the length of time that the phone is not used before the idle display XML service is invoked:
  - For a single phone—Idle Timer field on the Cisco Unified Communications Manager Phone configuration window
  - For multiple phones simultaneously—URL Idle Time field on the Cisco Unified Communications Manager Enterprise Parameters configuration window, or the Idle Timer field in the Bulk Administration Tool (BAT)

From a phone, you can see settings for the idle display XML service URL and the length of time that the phone is not used before this service is invoked. To see these settings, choose **Settings > Device Configuration** and scroll to the Idle URL and the Idle URL Time parameters.

Automatically Disabling the Cisco Unified IP Phone Touchscreen

To conserve power and ensure the longevity of the LCD screen on the phone, you can set the LCD to turn off when it is not needed.

You can configure settings in Cisco Unified Communications Manager Administration to turn off the display at a designated time on some days and all day on other days. For example, you may choose to turn off the display after business hours on weekdays and all day on Saturdays and Sundays.

When the display is off, the LCD screen is dark and disabled, and the **Display** button lights. You can take any of these actions to turn on the display any time it is off:

- Press any button on the phone.

  If you press a button other than the **Display** button, the phone will take the action designated by that button in addition to turning on the display.
- Touch the touchscreen.
- Lift the handset.

When you turn the display on, it remains on until the phone has remained idle for a designated length of time, then it turns off automatically.

Note You can use the **Display** button to temporarily disable the touchscreen for cleaning. See the "Cleaning the Cisco Unified IP Phone" section on page 9-17 for more information.

Table 6-1 explains the Cisco Unified Communications Manager Administration fields that control when the display turns on and off. You configure these fields in Cisco Unified Communications Manager Administration in the Product Specific configuration window. (You access this window by choosing **Device > Phone** from Cisco Unified Communications Manager Administration.)

You can view the display settings for a phone from the Power Save Configuration menu on the phone. For more information, see the "Power Save Configuration Menu" section on page 4-22.

Table 6-1 Display On and Off Configuration Fields

Field	Description
Days Display Not Active	Days that the display does not turn on automatically at the time specified in the Display On Time field. Choose the day or days from the drop-down list. To choose more than one day, Ctrl-click each day that you want.
Display On Time	Time each day that the display turns on automatically (except on the days specified in the Days Display Not Active field). Enter the time in this field in 24 hour format, where 0:00 is midnight. For example, to automatically turn the display on at 7:00 a.m., (0700), enter **7:00**. To turn the display on at 2:00 p.m. (1400), enter **14:00**. If this field is blank, the display will automatically turn on at 0:00.
Display On Duration	Length of time that the display remains on after turning on at the time specified in the Display On Time field. Enter the value in this field in the format *hours*:*minutes*. For example, to keep the display on for 4 hours and 30 minutes after it turns on automatically, enter **4:30**. If this field is blank, the phone will turn off at the end of the day (0:00). **Note** If Display On Time is 0:00 and the display on duration is blank (or 24:00), the display will remain on continuously.

Table 6-1 Display On and Off Configuration Fields (continued)

Field	Description
Display Idle Timeout	Length of time that the phone is idle before the display turns off. Applies only when the display was off as scheduled and was turned on by an end-user (by pressing a button on the phone, touching the touchscreen, or lifting the handset). Enter the value in this field in the format *hours*:*minutes*. For example, to turn the display off when the phone is idle for 1 hour and 30 minutes after an end-user turns the display on, enter **1:30**. The default value is 0:30.
Display On When Incoming Call	Disable/enable automatic illumination of the LCD screen when a call is received. Default: Disabled

CHAPTER 7

Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone

This chapter describes how to use the following menus and screens on the Cisco Unified IP Phone 7970 Series to view model information, status messages, network statistics, and firmware information for the phone:

- Model Information screen—Displays hardware and software information about the phone. For more information, see the "Model Information Screen" section on page 7-2.
- Status menu—Provides access to screens that display the status messages, network statistics, and firmware versions. For more information, see the "Status Menu" section on page 7-3.
- Call Statistics screen—Displays counters and statistics for the current call. For more information, see the "Call Statistics Screen" section on page 7-13.

You can use the information on these screens to monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information, and obtain other related information, remotely through the phone's web page. For more information, see Chapter 8, "Monitoring the Cisco Unified IP Phone Remotely."

For more information about troubleshooting the Cisco Unified IP Phone 7970 Series, see Chapter 9, "Troubleshooting and Maintenance."

This chapter includes these topics:

- Model Information Screen, page 7-2
- Status Menu, page 7-3

Model Information Screen

The Model Information screen includes the options that are described in Table 7-1.

To display the Model Information screen, press the **Settings** button and then select **Model Information.**

To exit the Model Information screen, press the **Exit** softkey.

Table 7-1 Model Information Settings

Option	Description	To Change
Model Number	Model number of the phone.	Display only—Cannot configure.
MAC Address	MAC address of the phone.	Display only—Cannot configure.
Load File	Identifier of the factory-installed load running on the phone.	Display only—Cannot configure.
Boot Load ID	Identifier of the factory-installed load running on the phone.	Display only—Cannot configure.
Serial Number	Serial number of the phone.	Display only—Cannot configure.
CTL	Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone. If no CTL file is installed on the phone, this field displays No. (If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets.	For more information about this file, refer to *Cisco Unified Communications Manager Security Guide*.
MIC	Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the MIC for your phone, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified Communications Manager Security Guide*.
LSC	Indicates whether a locally significant certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the LSC for your phone, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified Communications Manager Security Guide*.
Call Control Protocol	Indicates whether the phone is running under SCCP or SIP.	See the "Using Cisco Unified IP Phones with Different Protocols" section on page 2-12.

Status Menu

To display the Status menu, press the **Settings** button and then select **Status.**

To exit the Status menu, press the **Exit** softkey.

The Status menu includes these options, which provide information about the phone and its operation:

- Status Messages—Displays the Status Messages screen, which shows a log of important system messages. For more information, see the "Status Messages Screen" section on page 7-3.
- Network Statistics—Displays the Network Statistics screen, which shows Ethernet traffic statistics. For more information, see the "Network Statistics Screen" section on page 7-9.
- Firmware Versions—Displays the Firmware Versions screen, which shows information about the firmware running on the phone. For more information, see the "Firmware Versions Screen" section on page 7-11.
- Expansion Module(s)—Displays the Expansion Module(s) screen, which shows information about the Cisco Unified IP Phone Expansion Module 7914, if connected to the phone. For more information, see the "Expansion Module(s) Screen" section on page 7-12.

Status Messages Screen

The Status Messages screen displays the 10 most recent status messages that the phone has generated. You can access this screen at any time, even if the phone has not finished starting up. Table 7-2 describes the status messages that might display. This table also includes actions you can take to address errors.

To display the Status Messages screen, follow these steps:

Procedure

Step 1 Press the **Settings** button.

Step 2 Select **Status.**

Step 3 Select **Status Messages.**

To remove current status messages, press the **Clear** softkey.

To exit the Status Messages screen, press the **Exit** softkey.

Table 7-2 Status Messages on the Cisco Unified IP Phone 7970 Series

Message	Description	Possible Explanation and Action
BootP server used	The phone obtained its IP address from a BootP server rather than a DHCP server.	None. This message is informational only.
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	The configuration file for a phone is created when the phone is added to the Cisco Unified Communications Manager database. If the phone has not been added to the Cisco Unified Communications Manager database, the TFTP server generates a `CFG File Not Found` response. • Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to auto-register. See the "Adding Phones with Cisco Unified Communications Manager Administration" section on page 2-12 for details. • If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check configuration of the TFTP server. See the "Network Configuration Menu" section on page 4-5 for details on assigning a TFTP server.
CFG TFTP Size Error	The configuration file is too large for file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTP directory. You should only copy files into this directory when the TFTP server software is shut down, otherwise the files may be corrupted.
CTL Installed	A certificate trust list (CTL) file is installed in the phone.	None. This message is informational only. For more information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*.
CTL update failed	The phone could not update its certificate trust list (CTL) file.	Problem with the CTL file on the TFTP server. For more information, refer to *Cisco Unified Communications Manager Security Guide*.

Table 7-2 Status Messages on the Cisco Unified IP Phone 7970 Series (continued)

Message	Description	Possible Explanation and Action
DHCP timeout	DHCP server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the DHCP server and the phone—Verify the network connections. • DHCP server is down—Check configuration of DHCP server. • Errors persist—Consider assigning a static IP address. See the "Network Configuration Menu" section on page 4-5 for details on assigning a static IP address.
Disabled	802.1X Authentication is disabled on the phone.	You can enable 802.1X authentication using the **Settings > Security Configuration > 802.1X Authentication** option on the phone. For more information, see the "802.1X Authentication and Status" section on page 4-31.
DNS timeout	DNS server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the DNS server and the phone—Verify the network connections. • DNS server is down—Check configuration of DNS server.
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	• Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS. • Consider using IP addresses rather than host names.
Duplicate IP	Another device is using the IP address assigned to the phone.	• If the phone has a static IP address, verify that you have not assigned a duplicate IP address. See the "Network Configuration Menu" section on page 4-5 section for details. • If you are using DHCP, check the DHCP server configuration.

Table 7-2 Status Messages on the Cisco Unified IP Phone 7970 Series (continued)

Message	Description	Possible Explanation and Action
Error update locale	One or more localization files could not be found in the TFTP directory or were not valid. The locale was not changed.	From Cisco Unified Operating System Administration, check that the following files are located within the subdirectories in TFTP File Management: • Located in subdirectory with same name as network locale: – tones.xml • Located in subdirectory with same name as user locale: – glyphs.xml – dictionary.xml – kate.xml
Failed	The phone attempted an 802.1X transaction but authentication failed.	Authentication typically fails because of one of the following: • No shared secret is configured in the phone or authentication server • The shared secret configured in the phone and the authentication server do not match • Phone has not been configured in the authentication server
File auth error	An error occurred when the phone tried to validate the signature of a signed file. This message includes the name of the file that failed.	• The file is corrupted. If the file is a phone configuration file, delete the phone from the Cisco Unified Communications Manager database using Cisco Unified Communications Manager Administration. Then add the phone back to the Cisco Unified Communications Manager database using Cisco Unified Communications Manager Administration. • There is a problem with the CTL file and the key for the server from which files are obtained is bad. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.
File not found	The phone cannot locate, on the TFTP server, the phone load file that is specified in the phone configuration file.	From Cisco Unified Operating System Administration, make sure that the phone load file is listed in TFTP File Management.
IP address released	The phone has been configured to release its IP address.	The phone remains idle until it is power cycled or you reset the DHCP address. See the "Network Configuration Menu" section on page 4-5 section for details.

Table 7-2 Status Messages on the Cisco Unified IP Phone 7970 Series (continued)

Message	Description	Possible Explanation and Action
Load Auth Failed	The phone could not load a configuration file.	Check that: • A good version of the configuration file exists on the applicable server. • The phone load being downloaded has not been altered or renamed. • Phone load type is compatible; for example, you cannot place a DEV load configuration file on a REL-signed phone.
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose **Device > Phone**). Verify that the load ID is entered correctly.
Load rejected HC	The application that was downloaded is not compatible with the phone's hardware.	Occurs if you were attempting to install a version of software on this phone that did not support hardware changes on this newer phone. Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose **Device > Phone**). Re-enter the load displayed on the phone. See the "Firmware Versions Screen" section on page 7-11 to verify the phone setting.
Load Server is invalid	Indicates an invalid TFTP server IP address or name in the Load Server option.	The Load Server setting is not valid. The Load Server specifies a TFTP server IP address or name from which the phone firmware can be retrieved for upgrades on the phones. Check the Load Server entry (from Cisco Unified Communications Manager Administration choose **Device > Phone**).
No CTL installed	A certificate trust list (CTL) file is not installed in the phone.	Occurs if security is not configured. If security is configured, CTL file does not exist on the TFTP server. For more information, refer to *Cisco Unified Communications Manager Security Guide*.
No default router	DHCP or static configuration did not specify a default router.	• If the phone has a static IP address, verify that the default router has been configured. See the "Network Configuration Menu" section on page 4-5 section for details. • If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.

Table 7-2 Status Messages on the Cisco Unified IP Phone 7970 Series (continued)

Message	Description	Possible Explanation and Action
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	• If the phone has a static IP address, verify that the DNS server has been configured. See the "Network Configuration Menu" section on page 4-5 section for details. • If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.
Programming Error	The phone failed during programming.	Attempt to resolve this error by power cycling the phone. If the problem persists, contact Cisco technical support for additional assistance.
Successful – MD5	The phone attempted an 802.1X transaction and authentication achieved.	The phone achieved 802.1X authentication.
TFTP access error	TFTP server is pointing to a directory that does not exist.	• If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check configuration of TFTP server. See the "Network Configuration Menu" section on page 4-5 for details on assigning a TFTP server.
TFTP Error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.
TFTP file not found	The requested load file (.bin) was not found in the TFTP directory.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose **Device > Phone**). Verify that the TFTP directory contains a .bin file with this load ID as the name.
TFTP server not authorized	The specified TFTP server could not be found in the phone's CTL.	• The DHCP server has the wrong configuration file for the TFTP server. In this case, update the TFTP server configuration to specify the correct TFTP server. The CTL file was made and then the TFTP server address changed. In this case, regenerate the CTL file. • If the phone is using a static IP address, the phone may be configured with the wrong TFTP server address. In this case, enter the correct TFTP server address in the Network Configuration menu on the phone. • If the TFTP server address is correct, there may be a problem with the CTL file. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.

Table 7-2 Status Messages on the Cisco Unified IP Phone 7970 Series (continued)

Message	Description	Possible Explanation and Action
TFTP timeout	TFTP server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the TFTP server and the phone—Verify the network connections. • TFTP server is down—Check configuration of TFTP server.
Timed Out	Supplicant attempted 802.1X transaction but timed out due the absence of an authenticator.	Authentication typically times out if 802.1X authentication is not configured on the switch.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This is an informational message indicating the name of the configuration file for the phone.

Network Statistics Screen

The Network Statistics screen displays information about the phone and network performance. Table 7-3 describes the information that displays in this screen.

To display the Network Statistics screen, follow these steps:

Procedure

Step 1 Press the **Settings** button.

Step 2 Select **Status.**

Step 3 Select **Network Statistics.**

To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press the **Clear** softkey.

To exit the Network Statistics screen, press the **Exit** softkey.

Table 7-3 Network Statistics Message Components

Item	Description
Rx Frames	Number of packets received by the phone
Tx Frames	Number of packets sent by the phone
Rx Broadcasts	Number of broadcast packets received by the phone

Table 7-3 Network Statistics Message Components (continued)

Item	Description
One of the following values: Initialized TCP-timeout CM-closed-TCP TCP-Bad-ACK CM-reset-TCP CM-aborted-TCP CM-NAKed KeepaliveTO Failback Phone-Keypad Phone-Re-IP Reset-Reset Reset-Restart Phone-Reg-Rej Load Rejected HC CM-ICMP-Unreach Phone-Abort	Cause of the last reset of the phone
Elapsed Time	Amount of time that has elapsed since the phone last rebooted
Port 1	Link state and connection of the PC port (for example, `Auto 100 Mb Full-Duplex` means that the PC port is in a link-up state and has auto-negotiated a full-duplex, 100-Mbps connection)

Table 7-3 Network Statistics Message Components (continued)

Item	Description
Port 2	Link state and connection of the Network port
IPv4	Information on the DHCP status. This includes the following states: • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • SET DHCP COLDBOOT • SET DHCP DISABLED • DISABLED DUPLICATE IP • SET DHCP FAST

Firmware Versions Screen

The Firmware Versions screen displays information about the firmware version that is running on the phone. Table 7-4 explains the information that is displayed on this screen.

To display the Firmware Version screen, follow these steps:

Procedure

Step 1 Press the **Settings** button.

Step 2 Select **Status.**

Step 3 Select **Firmware Versions.**

To exit the Firmware Version screen, press the **Exit** softkey.

Table 7-4 Firmware Version Information

Item	Description
Load File	Load file running on the phone
App Load ID	Identifies the JAR file running on the phone
JVM Load ID	Identifies the Java Virtual Machine (JVM) running on the phone
OS Load ID	Identifies the operating system running on the phone
Boot Load ID	Identifies the factory-installed load running on the phone
Expansion Module 1 Expansion Module 2	Identifies the load running on the Expansion Module(s), if connected to and SCCP phone
DSP Load ID	Identifies the digital signal processor (DSP) software version used

Expansion Module(s) Screen

The Expansion Module(s) screen displays information about each Cisco Unified IP Phone Expansion Module 7914 that is connected to the phone.

Table 7-5 explains the information that is displayed on this screen for each connected expansion module. You can use this information to troubleshoot the expansion module, if necessary. In the Expansion Module(s) screen, a statistic preceded by "A" is for the first expansion module. A statistic preceded by "B" is for the second expansion module.

To display the Expansion Module(s) screen, follow these steps:

Procedure

Step 1 Press the **Settings** button.

Step 2 Select **Status.**

Step 3 Select **Expansion Module(s).**

To exit the Expansion Module(s) screen, press the **Exit** softkey.

Table 7-5 Expansion Module Statistics

Item	Description
Link State	Overall expansion module status
RX Discarded Bytes	Number of bytes discarded due to errors
RX Length Err	Number of packets discarded due to improper length
RX Checksum Err	Number of packets discarded due to invalid checksum information
RX Invalid Message	Number of packets that have been discarded because a message was invalid or unsupported

Table 7-5 Expansion Module Statistics (continued)

Item	Description
TX Retransmit	Number of packets that have been retransmitted to the expansion module
TX Buffer Full	Number of packets discarded because the expansion module was not able to accept new messages

Call Statistics Screen

The Call Statistics screen displays counters statistics and voice-quality metrics in these ways:

- During call—You can view the call information by rapidly pressing the *?* button twice.
- After the call—You can view the call information captured during the last call by displaying the Call Statistics screen.

Note You can also remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics not available on the phone. For more information about remote monitoring, see Chapter 8, "Monitoring the Cisco Unified IP Phone Remotely."

A single call can have multiple voice streams, but data is captured for only the last voice stream. A voice stream is a packet stream between two endpoints. If one endpoint is put on hold, the voice stream stops even though the call is still connected. When the call resumes, a new voice packet stream begins, and the new call data overwrites the former call data.

To display the Call Statistics screen for information about the last voice stream, follow these steps:

Procedure

Step 1 Press the **Settings** button.

Step 2 Select **Status**.

Step 3 Select **Call Statistics**.

Table 7-6 explains the items displayed in the Call Statistics screen:

Table 7-6 Call Statistics Items

Item	Description
Rcvr Codec	Type of voice stream received (RTP streaming audio from codec): G.729, G.711 u-law, G.711 A-law, or Lin16k.
Sender Codec	Type of voice stream transmitted (RTP streaming audio from codec): G.729, G.728/iLBC, G.711 u-law, G.711 A-law, or Lin16k.
Rcvr Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).

Table 7-6 Call Statistics Items (continued)

Item	Description
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Rcvr Packets	Number of RTP voice packets received since voice stream was opened. **Note** This number is not necessarily identical to the number of RTP voice packets received since the call began because the call might have been placed on hold.
Sender Packets	Number of RTP voice packets transmitted since voice stream was opened. **Note** This number is not necessarily identical to the number of RTP voice packets transmitted since the call began because the call might have been placed on hold.
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened.
Max Jitter	Maximum jitter observed since the receiving voice stream was opened.
Rcvr Discarded	Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on). **Note** The phone will discard payload type 19 comfort noise packets that are generated by Cisco Gateways, which will increment this counter.
Rcvr Lost Packets	Missing RTP packets (lost in transit).
Voice Quality Metrics	
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see the "Monitoring the Voice Quality of Calls" section on page 9-15. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.722 gives 4.5 • G.728/iLBC gives 3.9 • G.729 A/AB gives 3.8

Table 7-6 Call Statistics Items (continued)

Item	Description
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Network Protocol	Identifies the current Network Protocol—IPv4.

CHAPTER 8

Monitoring the Cisco Unified IP Phone Remotely

Each Cisco Unified IP Phone has a web page from which you can view a variety of information about the phone, including:

- Device information
- Network configuration information
- Network statistics
- Device logs
- Streaming statistics

This chapter describes the information that you can obtain from the phone's web page. You can use this information to remotely monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information directly from a phone. For more information, see Chapter 7, "Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone."

For more information about troubleshooting the Cisco Unified IP Phone 7970 Series, see Chapter 9, "Troubleshooting and Maintenance."

This chapter includes these topics:

- Accessing the Web Page for a Phone, page 8-1
- Disabling and Enabling Web Page Access, page 8-3
- Device Information, page 8-3
- Network Configuration, page 8-4
- Network Statistics, page 8-8
- Device Logs, page 8-10
- Streaming Statistics, page 8-10

Accessing the Web Page for a Phone

To access the web page for a Cisco Unified IP Phone, perform these steps.

Note If you cannot access the web page, it may be disabled. See the "Disabling and Enabling Web Page Access" section on page 8-3 for more information.

Procedure

Step 1 Obtain the IP address of the Cisco Unified IP Phone by using one of these methods:

- Search for the phone in Cisco Unified Communications Manager by choosing **Device > Phone**. Phones registered with Cisco Unified Communications Manager display the IP address at the top of the Phone Configuration window.
- On the phone, press the **Settings** button, choose **Network Configuration**, and then scroll to the IP Address option.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco Unified IP Phone:

http://*IP_address*

The web page for a Cisco Unified IP Phone 7970 Series includes these hyperlinks:

- **Device Information**—Displays device settings and related information for the phone. For more information, see the "Device Information" section on page 8-3.
- **Network Configuration**—Displays network configuration information and information about other phone settings. For more information, see the "Network Configuration" section on page 8-4.
- **Network Statistics**—Includes the following hyperlinks, which provide information about network traffic:
  - **Ethernet Information**—Displays information about Ethernet traffic. For more information, see the "Network Statistics" section on page 8-8.
  - **Access**—Displays information about network traffic to and from the PC port on the phone. For more information, see the "Network Statistics" section on page 8-8.
  - **Network**—Displays information about network traffic to and from the network port on the phone. For more information, see the "Network Statistics" section on page 8-8.
- **Device Logs**—Includes the following hyperlinks, which provide information that you can use for troubleshooting:
  - **Console Logs**—Includes hyperlinks to individual log files. For more information, see the "Device Logs" section on page 8-10.
  - **Core Dumps**—Includes hyperlinks to individual dump files.
  - **Status Messages**—Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. For more information, see the "Device Logs" section on page 8-10.
  - **Debug Display**—Displays messages that might be useful to the Cisco TAC if you require assistance with troubleshooting. For more information, see the "Device Logs" section on page 8-10.
- **Streaming Statistics**—Includes the **Stream 1**, **Stream 2**, and **Stream 3** hyperlinks, which display a variety of streaming statistics. For more information, see the "Streaming Statistics" section on page 8-10.

Disabling and Enabling Web Page Access

For security purposes, you may choose to prevent access to the web pages for a phone. If you do so, you will prevent access to the web pages that are described in this chapter and to the phone's User Options web pages.

To control access to the web pages for a phone, follow these steps from Cisco Unified Communications Manager Administration:

Step 1 Choose **Device > Phone**.

Step 2 Specify the criteria to find the phone and click **Find**, or click **Find** to display a list of all phones.

Step 3 Click the device name to open the Phone Configuration window for the device.

Step 4 From the Web Access drop-down list box, choose one of these options:

- **Disabled**—Prevents access to web pages for a phone.
- **Enabled**—Allows access to web pages for a phone.

Step 5 Click **Update**.

Note Some features, such as Cisco Quality Report Tool, do not function properly without access to the phone web pages. Disabling web access also affects any serviceability application that relies on web access.

Device Information

The Device Information area on a phone's web page displays device settings and related information for the phone. Table 8-1 describes these items.

To display the Device Information area, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 8-1, and then click the **Device Information** hyperlink.

Table 8-1 Device Information Area Items

Item	Description
MAC Address	Media Access Control (MAC) address of the phone
Host Name	Unique, fixed name that is automatically assigned to the phone based on its MAC address
Phone DN	Directory number assigned to the phone
App Load ID	Identifier of the firmware running on the phone
Boot Load ID	Identifier of the factory-installed load running on the phone
Version	Version of the firmware running on the phone
Expansion Module 1	Phone load ID for the first Cisco Unified IP Phone Expansion Module 7914
Expansion Module 2	Phone load ID for the second Cisco Unified IP Phone Expansion Module 7914
Hardware Revision	Revision value of the phone hardware

Table 8-1 Device Information Area Items (continued)

Item	Description
Serial Number	Serial number of the phone
Model Number	Model number of the phone
Message Waiting	Indicates if there is a voice message waiting on any line for this phone
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: • Device Type—Indicates hardware type. For example, *phone* displays for all phone models • Device Description—Displays the name of the phone that is associated with the indicated model type • Product Identifier—Specifies the phone model • Version Identifier[1]—Represents the hardware version of the phone • Serial Number—Displays the phone's unique serial number
Time	Time obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs
Time Zone	Timezone obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs
Date	Date obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs

1. The Version Identifier field might display blank if using an older model Cisco Unified IP Phone because the hardware does not provide this information.

Network Configuration

The Network Configuration area on a phone's web page displays network configuration information and information about other phone settings. Table 8-2 describes this information.

You can view and set many of these items from the Network Configuration Menu and the Device Configuration Menu on the Cisco Unified IP Phone. For more information, see Chapter 5, "Configuring Features, Templates, Services, and Users."

To display the Network Configuration area, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 8-1, and then click the **Network Configuration** hyperlink.

Table 8-2 Network Configuration Area Items

Item	Description
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Host name that the DHCP server assigned to the phone.

Table 8-2 Network Configuration Area Items (continued)

Item	Description
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.
IP Address	Internet Protocol (IP) address of the phone.
Subnet Mask	Subnet mask used by the phone.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone.
Default Router 1–5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5.
DNS Server 1–5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.
Admin. VLAN ID	Auxiliary VLAN in which the phone is a member.
Unified CM 1–5	Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Manager servers with which the phone can register. An item can also show the IP address of an SRST router that is capable of providing limited Cisco Unified Communications Manager functionality, if such a router is available. For an available server, an item will show the Cisco Unified Communications Manager server IP address and one of the following states: • Active—Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services. • Standby—Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable. • Blank—No current connection to this Cisco Unified Communications Manager server. An item may also include the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. You configure the SRST router address in the Device Pool section in Cisco Unified Communications Manager Configuration window.
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.

Table 8-2 Network Configuration Area Items (continued)

Item	Description
DHCP Enabled	Indicates whether DHCP is being used by the phone.
DHCP Address Released	Indicates the setting of the DHCP Address Released option on the phone's Network Configuration menu.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.
Idle URL	URL that the phone displays when the phone has not been used for the time specified by Idle URL Time, and no menu is open.
Idle URL Time	Number of seconds that the phone has not been used and no menu is open before the XML service specified by Idle URL is activated.
Proxy Server URL	URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the phone HTTP client and provides responses from the non-local host to the phone HTTP client.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.
SW Port Configuration	Speed and duplex of the switch port, where: • A—Auto Negotiate • 10H—10-BaseT/half duplex • 10F—10-BaseT/full duplex • 100H—100-BaseT/half duplex • 100F—100-BaseT/full duplex • 1000H—1000-BaseT/half duplex • 1000F—1000-BaseT/full duplex • No Link—No connection to the switch port
PC Port Configuration	Speed and duplex of the switch port, where: • A—Auto Negotiate • 10H—10-BaseT/half duplex • 10F—10-BaseT/full duplex • 100H—100-BaseT/half duplex • 100F—100-BaseT/full duplex • 1000H—1000-BaseT/half duplex • 1000F—1000-BaseT/full duplex • No Link—No connection to the PC port
TFTP Server 2	Backup TFTP server that the phone uses if the primary TFTP server is unavailable.
User Locale	User locale associated with the phone user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale associated with the phone user. Identifies a set of detailed information to support the phone in a specific location, including definitions of the tones and cadences used by the phone.

Table 8-2 Network Configuration Area Items (continued)

Item	Description
Headset enabled	Indicates whether the Headset button is enabled on the phone.
User Locale Version	Version of the user locale loaded on the phone.
Network Locale Version	Version of the network locale loaded on the phone.
PC Port Disabled	Indicates whether the PC port on the phone is enabled or disabled.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Video Capability Enabled	Indicates whether the phone can participate in video calls when connected to an appropriately equipped PC.
Voice VLAN Enabled	Indicates whether the phone allows a device attached to the PC port to access the Voice VLAN.
Auto Line Select	Indicates whether the phone shifts the call focus to incoming calls on all lines.
DSCP for Call Control	DSCP IP classification for call control signaling.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based services.
Security Mode	Displays the security mode that is set for the phone.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.
Span to PC Port	Indicates whether the phone will forward packets transmitted and received on the network port to the access port.
PC VLAN	VLAN used to identify and remove 802.1P/Q tags from packets sent to the PC.
CDP: PC Port	Indicates whether CDP is supported on the PC port.
CDP: SW Port	Indicates whether CDP is supported on the switch xport.
LLDP-MED: SW Port	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.
LLDP: PC Port	Indicates whether Link Layer Discovery Protocol (LLDP) is enabled on the PC port.
LLDP Power Priority	Advertises the phone's power priority to the switch, enabling the switch to appropriately provide power to the phones. Settings include: • Unknown—default • Low • High • Critical
LLDP Asset ID	Identifies the asset ID assigned to the phone for inventory management.

Network Statistics

These network statistics areas on a phone's web page provide information about network traffic on the phone:

- Ethernet Information area—Displays information about Ethernet traffic. Table 8-3 describes the items in this area.
- Access area—Displays information about network traffic to and from the PC port on the phone. Table 8-4 describes the items in this area.
- Network area—Displays information about network traffic to and from the network port on the phone. Table 8-4 describes the items in this area.

To display a network statistics area, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 8-1, and then click the **Ethernet Information**, the **Access**, and or the **Network** hyperlink.

Table 8-3 Ethernet Information Area Items

Item	Description
Tx Frames	Total number of packets transmitted by the phone
Tx broadcast	Total number of broadcast packets transmitted by the phone
Tx multicast	Total number of multicast packets transmitted by the phone
Tx unicast	Total number of unicast packets transmitted by the phone
Rx Frames	Total number of packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone
Rx multicast	Total number of multicast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
RxPacketNoDes	Total number of shed packets caused by no Direct Memory Access (DMA) descriptor

Table 8-4 Access Area and Network Area Items

Item	Description
Rx totalPkt	Total number of packets received by the phone
Rx crcErr	Total number of packets received with CRC failed
Rx alignErr	Total number of packets received between 64 and 1522 bytes in length that have a bad Frame Check Sequence (FCS)
Rx multicast	Total number of multicast packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
Rx shortErr	Total number of FCS error packets or Align error packets received that are less than 64 bytes in size
Rx shortGood	Total number of good packets received that are less than 64 bytes size
Rx longGood	Total number of good packets received that are greater than 1522 bytes in size

Table 8-4 Access Area and Network Area Items (continued)

Item	Description
Rx longErr	Total number of FCS error packets or Align error packets received that are greater than 1522 bytes in size
Rx size64	Total number of packets received, including bad packets, that are between 0 and 64 bytes in size
Rx size65to127	Total number of packets received, including bad packets, that are between 65 and 127 bytes in size
Rx size128to255	Total number of packets received, including bad packets, that are between 128 and 255 bytes in size
Rx size256to511	Total number of packets received, including bad packets, that are between 256 and 511 bytes in size
Rx size512to1023	Total number of packets received, including bad packets, that are between 512 and 1023 bytes in size
Rx size1024to1518	Total number of packets received, including bad packets, that are between 1024 and 1518 bytes in size
Rx tokenDrop	Total number of packets dropped due to lack of resources (for example, FIFO overflow)
Tx excessDefer	Total number of packets delayed from transmitting due to medium being busy
Tx lateCollision	Number of times that collisions occurred later than 512 bit times after the start of packet transmission
Tx totalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) received by the phone
Tx Collisions	Total number of collisions that occurred while a packet was being transmitted
Tx excessLength	Total number of packets not transmitted because the packet experienced 16 transmission attempts
Tx broadcast	Total number of broadcast packets transmitted by the phone
Tx multicast	Total number of multicast packets transmitted by the phone
LLDP FramesOutTotal	Total number of LLDP frames sent out from the phone
LLDP AgeoutsTotal	Total number of LLDP frames that have been time out in cache
LLDP FramesDiscardedTotal	Total number of LLDP frames that are discarded when any of the mandatory TLVs is missing or out of order or contains out of range string length.
LLDP FramesInErrorsTotal	Total number of LLDP frames that received with one or more detectable errors
LLDP FramesInTotal	Total number of LLDP frames received on the phone.
LLDP TLVDiscardedTotal	Total number of LLDP TLVs that are discarded.
LLDP TLVUnrecognizedTotal	Total number of LLDP TLVs that are not recognized on the phone.
CDP Neighbor Device ID	Identifier of a device connected to this port discovered by CDP protocol.

Table 8-4 Access Area and Network Area Items (continued)

Item	Description
CDP Neighbor IP Address	IP address of the neighbor device discovered by CDP protocol.
CDP Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protocol.
LLDP Neighbor Device ID	Identifier of a device connected to this port discovered by LLDP protocol.
LLDP Neighbor IP Address	IP address of the neighbor device discovered by LLDP protocol.
LLDP Neighbor Port	Neighbor device port to which the phone is connected discovered by LLDP protocol.

Device Logs

The Device Logs area on a phone's web page provides information you can use to help monitor and troubleshoot the phone.

- Console Logs—Includes hyperlinks to individual log files. The console log files include debug and error messages received on the phone.
- Core Dumps—Includes hyperlinks to individual dump files.
- Status Messages area—Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. You can also see this information from the Status Messages screen on the phone. Table 7-2 describes the status messages that can appear.

  To display the Status Messages, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 8-1, and then click the **Status Messages** hyperlink.
- Debug Display area—Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

Streaming Statistics

A Cisco Unified IP Phone can stream information to and from up to three devices simultaneously. A phone streams information when it is on a a call or running a service that sends or receives audio or data.

The streaming statistics areas on a phone's web page provide information about the streams. Most calls use only one stream (Stream 1), but some calls use two or three stream. For example, a barged call uses Stream 1 and Stream 2.

To display a Streaming Statistics area, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 8-1, and then click the **Stream 1**, the **Stream 2**, or the **Stream 3** hyperlink.

Table 8-5 describes the items in the Streaming Statistics areas.

Table 8-5 Streaming Statistics Area Items

Item	Description
Remote Address	IP address and UDP port of the destination of the stream.
Local Address	IP address and UPD port of the phone.

Table 8-5 Streaming Statistics Area Items (continued)

Item	Description
Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requested that the phone start transmitting packets.
Stream Status	Indication of whether streaming is active or not.
Host Name	Unique, fixed name that is automatically assigned to the phone based on its MAC address.
Sender Packets	Total number of RTP data packets transmitted by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Octets	Total number of payload octets transmitted in RTP data packets by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Codec	Type of audio encoding used for the transmitted stream.
Sender Reports Sent[1]	Number of times the RTCP Sender Reports have been sent.
Sender Report Time Sent[1]	Internal time stamp indicating when a RTCP Sender Report was sent.
Rcvr Lost Packets	Total number of RTP data packets that have been lost since starting receiving data on this connection. Defined as the number of expected packets less the number of packets actually received, where the number of received packets includes any that are late or duplicate. The value displays as 0 if the connection was set to send-only mode.
Avg Jitter	Estimate of mean deviation of the RTP data packet inter-arrival time, measured in milliseconds. The value displays as 0 if the connection was set to send-only mode.
Rcvr Codec	Type of audio encoding used for the received stream.
Rcvr Reports Sent[1]	Number of times the RTCP Receiver Reports have been sent.
Rcvr Report Time Sent[1]	Internal time stamp indicating when a RTCP Receiver Report was sent.
Rcvr Packets	Total number of RTP data packets received by the phone since starting receiving data on this connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Rcvr Octets	Total number of payload octets received in RTP data packets by the device since starting reception on the connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see the "Monitoring the Voice Quality of Calls" section on page 9-15. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.

Table 8-5 Streaming Statistics Area Items (continued)

Item	Description
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.729 A /AB gives 3.7
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency[1]	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.
Sender Reports Received[1]	Number of times RTCP Sender Reports have been received.
Sender Report Time Received[1]	Last time at which an RTCP Sender Report was received.
Rcvr Size	RTP packet size, in milliseconds, for the received stream.
Rcvr Discarded	RTP packets received from network but discarded from jitter buffers.
Rcvr Reports Received[1]	Number of times RTCP Receiver Reports have been received.
Rcvr Report Time Received[1]	Last time at which an RTCP Receiver Report was received.
Voice Quality Metrics	
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see the "Monitoring the Voice Quality of Calls" section on page 9-15. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.

Table 8-5 Streaming Statistics Area Items (continued)

Item	Description
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.729 A /AB gives 3.7
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
Cmltve Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.

1. When the RTP Control Protocol is disabled, no data generates for this field and thus displays as 0.

Related Topics

- "Configuring Settings on the Cisco Unified IP Phone" chapter
- "Configuring Features, Templates, Services, and Users" chapter
- "Call Statistics Screen" section on page 7-13
- "Monitoring the Voice Quality of Calls" section on page 9-15

CHAPTER 9

Troubleshooting and Maintenance

This chapter provides information that can assist you in troubleshooting problems with your Cisco Unified Unified IP Phone 7970 Series or with your IP telephony network. It also explains how to clean and maintain your phone.

For additional troubleshooting information, refer to the *Using the 79xx Status Information For Troubleshooting* tech note. That document is available to registered Cisco.com users at this URL:

http://www.cisco.com/warp/customer/788/AVVID/telecaster_trouble.html

If you need additional assistance to resolve an issue, see the "Obtaining Documentation, Obtaining Support, and Security Guidelines" section on page xiii.

This chapter includes these topics:

- Resolving Startup Problems, page 9-1
- Cisco Unified IP Phone Resets Unexpectedly, page 9-6
- Troubleshooting Cisco Unified IP Phone Security, page 9-8
- General Troubleshooting Tips, page 9-10
- General Troubleshooting Tips for the Cisco Unified IP Phone Expansion Module 7914, page 9-12
- Resetting or Restoring the Cisco Unified IP Phone, page 9-13
- Using the Quality Report Tool, page 9-14
- Monitoring the Voice Quality of Calls, page 9-15
- Where to Go for More Troubleshooting Information, page 9-17
- Cleaning the Cisco Unified IP Phone, page 9-17

Resolving Startup Problems

After installing a Cisco Unified IP Phone into your network and adding it to Cisco Unified Communications Manager, the phone should start up as described in the "Verifying the Phone Startup Process" section on page 3-10. If the phone does not start up properly, see the following sections for troubleshooting information:

- Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process, page 9-2
- Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager, page 9-2
- Symptom: Cisco Unified IP Phone Unable to Obtain IP Address, page 9-6

Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process

When you connect a Cisco Unified IP Phone into the network port, the phone should go through its normal startup process as described in the "Verifying the Phone Startup Process" section on page 3-10, and the LCD screen should display information. If the phone does not go through the startup process, the cause may be faulty cables, bad connections, network outages, lack of power, and so on. Or, the phone may not be functional.

To determine whether the phone is functional, follow these suggestions to systematically eliminate these other potential problems:

1. Verify that the network port is functional:
   - Exchange the Ethernet cables with cables that you know are functional.
   - Disconnect a functioning Cisco Unified IP Phone from another port and connect it to this network port to verify the port is active.
   - Connect the Cisco Unified IP Phone that will not start up to a different network port that is known to be good.
   - Connect the Cisco Unified IP Phone that will not start up directly to the port on the switch, eliminating the patch panel connection in the office.
2. Verify that the phone is receiving power:
   - If you are using external power, verify that the electrical outlet is functional.
   - If you are using in-line power, use the external power supply instead.
   - If you are using the external power supply, switch with a unit that you know to be functional.
   - If you are using a Cisco Unified IP Phone 7971G-GE, make sure that the phone is connected to a switch that supports IEEE 802.3af Class 3 (15.4 W in-line power at the switch port). For more information, see the "Providing Power to the Phone" section on page 2-3.
3. If the phone still does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.
4. If the phone still does not start up properly, perform a factory reset of the phone. For instructions, see the "Performing a Factory Reset" section on page 9-14.

If after attempting these solutions, the LCD screen on the Cisco Unified IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager

If the phone proceeds past the first stage of the startup process (LED buttons flashing on and off) but continues to cycle through the messages displaying on the LCD screen, the phone is not starting up properly. The phone cannot successfully start up unless it is connected to the Ethernet network and it has registered with a Cisco Unified Communications Manager server.

These sections can assist you in determining the reason the phone is unable to start up properly:

- Identifying Error Messages, page 9-3
- Checking Network Connectivity, page 9-3

- Verifying TFTP Server Settings, page 9-3
- Verifying IP Addressing and Routing, page 9-3
- Verifying DNS Settings, page 9-4
- Verifying Cisco Unified Communications Manager Settings, page 9-4
- Cisco CallManager and TFTP Services Are Not Running, page 9-4
- Creating a New Configuration File, page 9-5
- Registering the Phone with Cisco Unified Communications Manager, page 9-5

Identifying Error Messages

As the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem. See the "Status Messages Screen" section on page 7-3 for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Checking Network Connectivity

If the network is down between the phone and the TFTP server or Cisco Unified Communications Manager, the phone cannot start up properly. Ensure that the network is currently running.

Verifying TFTP Server Settings

You can determine the IP address of the TFTP server used by the phone by pressing the **Settings** button on the phone, choosing **Network Configuration > IPv4**, and scrolling to the **TFTP Server 1** option.

If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option. See the "Network Configuration Menu" section on page 4-5.

If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check the IP address configured in Option 150.

You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone was recently moved from one location to another. See the "Network Configuration Menu" section on page 4-5 for instructions.

Verifying IP Addressing and Routing

You should verify the IP addressing and routing settings on the phone. If you are using DHCP, the DHCP server should provide these values. If you have assigned a static IP address to the phone, you must enter these values manually.

On the Cisco Unified IP Phone, press the **Settings** button, choose **Network Configuration**, and look at the following options:

- DHCP Server—If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If it does not, check your IP routing and VLAN configuration. Refer to *Troubleshooting Switch Port Problems*, available at this URL: http://www.cisco.com/warp/customer/473/53.shtml
- IP Address, Subnet Mask, Default Router—If you have assigned a static IP address to the phone, you must manually enter settings for these options. See the "Network Configuration Menu" section on page 4-5 for instructions.

If you are using DHCP, check the IP addresses distributed by your DHCP server. Refer to *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks*, available at this URL: http://www.cisco.com/warp/customer/473/100.html#41

Verifying DNS Settings

If you are using DNS to refer to the TFTP server or to Cisco Unified Communications Manager, you must ensure that you have specified a DNS server. Verify this setting by pressing the **Settings** button on the phone, choosing **Network Configuration,** and scrolling to the **DNS Server 1** option. You should also verify that there is a CNAME entry in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.

You must also ensure that DNS is configured to do reverse look-ups.

Verifying Cisco Unified Communications Manager Settings

On the Cisco Unified IP Phone, press the **Settings** button, choose **Device Configuration**, and look at the **Unified CM Configuration** options. The Cisco Unified IP Phone attempts to open a TCP connection to all the Cisco Unified Communications Manager servers that are part of the assigned Cisco Unified Communications Manager group. If none of these options contain IP addresses or show Active or Standby, the phone is not properly registered with Cisco Unified Communications Manager. See the "Registering the Phone with Cisco Unified Communications Manager" section on page 9-5 for tips on resolving this problem.

Cisco CallManager and TFTP Services Are Not Running

If the Cisco CallManager or TFTP services are not running, phones may not be able to start up properly. However, in such a situation, it is likely that you are experiencing a system-wide failure, and that other phones and devices are unable to start up properly.

If the Cisco CallManager service is not running, all devices on the network that rely on it to make phone calls will be affected. If the TFTP service is not running, many devices will not be able to start up successfully.

To start a service, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list.

Step 2 Choose **Tools > Control Center - Network Services**.

Step 3 Choose the primary Cisco Unified Communications Manager server from the Server drop-down list.

The window displays the service names for the server that you chose, the status of the services, and a service control panel to stop or start a service.

Step 4 If a service has stopped, click its radio button and then click the **Start** button.

The Service Status symbol changes from a square to an arrow.

Note A service must be activated before it can be started or stopped. To activate a service, choose **Tools > Service Activation**.

Creating a New Configuration File

If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.

To create a new configuration file, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager, choose **Device > Phone > Find** to locate the phone experiencing problems.

Step 2 Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.

Step 3 Add the phone back to the Cisco Unified Communications Manager database. See the "Adding Phones to the Cisco Unified Communications Manager Database" section on page 2-9 for details.

Step 4 Power cycle the phone.

Note

- When you remove a phone from the Cisco Unified Communications Manager database, its configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone's directory number or numbers remain in the Cisco Unified Communications Manager database. They are called "unassigned DNs" and can be used for other devices. If unassigned DNs are not used by other devices, delete them from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. Refer to Cisco Unified Communications Manager Administration Guide for more information.
- Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but there is no button on the phone with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

Registering the Phone with Cisco Unified Communications Manager

A Cisco Unified IP Phone can register with a Cisco Unified Communications Manager server only if the phone has been added to the server or if auto-registration is enabled. Review the information and procedures in the "Adding Phones to the Cisco Unified Communications Manager Database" section on page 2-9 to ensure that the phone has been added to the Cisco Unified Communications Manager database.

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device > Phone > Find** from Cisco Unified Communications Manager Administration to search for the phone based on its MAC Address. For information about determining a MAC address, see the "Determining the MAC Address of a Cisco Unified IP Phone" section on page 2-14.

If the phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged. See the "Creating a New Configuration File" section on page 9-5 for assistance.

Symptom: Cisco Unified IP Phone Unable to Obtain IP Address

If a phone is unable to obtain an IP address when it starts up, the phone may be not be on the same network or VLAN as the DHCP server, or the switch port to which the phone is connected may be disabled.

Make sure that the network or VLAN to which the phone is connected has access to the DHCP server, and make sure that the switch port is enabled.

Cisco Unified IP Phone Resets Unexpectedly

If users report that their phones are resetting during calls or while idle on their desk, you should investigate the cause. If the network connection and Cisco Unified Communications Manager connection are stable, a Cisco Unified IP Phone should not reset on its own.

Typically, a phone resets if it has problems connecting to the Ethernet network or to Cisco Unified Communications Manager. These sections can help you identify the cause of a phone resetting in your network:

- Verifying Physical Connection, page 9-6
- Identifying Intermittent Network Outages, page 9-6
- Verifying DHCP Settings, page 9-7
- Checking Static IP Address Settings, page 9-7
- Verifying Voice VLAN Configuration, page 9-7
- Verifying that the Phones Have Not Been Intentionally Reset, page 9-7
- Eliminating DNS or Other Connectivity Errors, page 9-7
- Checking Power Connection, page 9-8

Verifying Physical Connection

Verify that the Ethernet connection to which the Cisco Unified IP Phone is connected is up. For example, check whether the particular port or switch to which the phone is connected is down and that the switch is not rebooting. Also make sure that there are no cable breaks.

Identifying Intermittent Network Outages

Intermittent network outages affect data and voice traffic differently. Your network might have been experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect its network connection.

If you are experiencing problems with the voice network, you should investigate whether an existing problem is simply being exposed.

Verifying DHCP Settings

Follow this process to help determine if the phone has been properly configured to use DHCP:

1. Verify that you have properly configured the phone to use DHCP. See the "Network Configuration Menu" section on page 4-5 for more information.
2. Verify that the DHCP server has been set up properly.
3. Verify the DHCP lease duration. Cisco recommends that you set it to 8 days.

   Cisco Unified IP Phones send messages with request type 151 to renew their DHCP address leases. If the DHCP server expects messages with request type 150, the lease will be denied, forcing the phone to restart and request a new IP address from the DHCP server.

Checking Static IP Address Settings

If the phone has been assigned a static IP address, verify that you have entered the correct settings. See the "Network Configuration Menu" section on page 4-5 for more information.

Verifying Voice VLAN Configuration

If the Cisco Unified IP Phone appears to reset during heavy network usage (for example, following extensive web surfing on a computer connected to same switch as phone), it is likely that you do not have a voice VLAN configured.

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic. See the "Understanding How the Cisco Unified IP Phone Interacts with the VLAN" section on page 2-3 for details.

Verifying that the Phones Have Not Been Intentionally Reset

If you are not the only administrator with access to Cisco Unified Communications Manager, you should verify that no one else has intentionally reset the phones.

You can check whether a Cisco Unified IP Phone received a command from Cisco Unified Communications Manager to reset by pressing the **Settings** button on the phone and choosing **Status > Network Statistics**. If the phone was recently reset one of these messages appears:

- Reset-Reset—Phone closed due to receiving a Reset/Reset from Cisco Unified Communications Manager Administration.
- Reset-Restart—Phone closed due to receiving a Reset/Restart from Cisco Unified Communications Manager Administration.

Eliminating DNS or Other Connectivity Errors

If the phone continues to reset, follow these steps to eliminate DNS or other connectivity errors:

Procedure

Step 1 Use the **Erase** softkey to reset phone settings to their default values. See the "Resetting or Restoring the Cisco Unified IP Phone" section on page 9-13 for details.

Step 2 Modify DHCP and IP settings:

a. Disable DHCP. See the "Network Configuration Menu" section on page 4-5 for instructions.

b. Assign static IP values to the phone. See the "Network Configuration Menu" section on page 4-5 for instructions. Use the same default router setting used for other functioning Cisco Unified IP Phones.

c. Assign TFTP server. See the "Network Configuration Menu" section on page 4-5 for instructions. Use the same TFTP server used for other functioning Cisco Unified IP Phones.

Step 3 On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.

Step 4 From Cisco Unified Communications Manager, choose **System > Server** and verify that the server is referred to by its IP address and not by its DNS name.

Step 5 From Cisco Unified Communications Manager, choose **Device > Phone** and verify that you have assigned the correct MAC address to this Cisco Unified IP Phone. For information about determining a MAC address, see the "Determining the MAC Address of a Cisco Unified IP Phone" section on page 2-14.

Step 6 Power cycle the phone.

Checking Power Connection

In most cases, a phone will restart if it powers up by using external power but loses that connection and switches to PoE. Similarly, a phone may restart if it powers up by using PoE and then gets connected to an external power supply.

Troubleshooting Cisco Unified IP Phone Security

Table 9-1 provides troubleshooting information for the security features on the Cisco Unified IP Phone. For information relating to the solutions for any of these issues, and for additional troubleshooting information about security, refer to *Cisco Unified Communications Manager Security Guide*.

Table 9-1 Cisco Unified IP Phone Security Troubleshooting

Problem	Possible Cause
CTL File Problems	
Device authentication error.	CTL file does not have a Cisco Unified Communications Manager certificate or has an incorrect certificate.
Phone cannot authenticate CTL file.	The security token that signed the updated CTL file does not exist in the CTL file on the phone.
Phone cannot authenticate any of the configuration files other than the CTL file.	There is a bad TFTP record.

Table 9-1 Cisco Unified IP Phone Security Troubleshooting (continued)

Problem	Possible Cause
Phone reports TFTP authorization failure.	• The TFTP address for the phone does not exist in the CTL file. • If you created a new CTL file with a new TFTP record, the existing CTL file on the phone may not contain a record for the new TFTP server.
Phone does not register with Cisco Unified Communications Manager.	The CTL file does not contain the correct information for the Cisco Unified Communications Manager server.
Phone does not request signed configuration files.	The CTL file does not contain any TFTP entries with certificates.
802.1X Enabled on Phone but Not Authenticating	
Phone cannot obtain a DHCP-assigned IP address. Phone does not register with Cisco Unified Communications Manager. Phone status display as "Configuring IP" or "Registering". 802.1X Authentication Status displays as "Held" (see the "802.1X Authentication and Status" section on page 4-31 for more details). Status menu displays 802.1X status as "Failed" (see the "Status Menu" section on page 7-3 for more details).	These errors typically indicate that 802.1X authentication is enabled on the phone, but the phone is unable to authenticate. 1. Verify that you have properly configured the required components (see the "Supporting 802.1X Authentication on Cisco Unified IP Phones" section on page 1-16 for more information). 2. Confirm that the shared secret is configured on the phone (see the"802.1X Authentication and Status" section on page 4-31 for more information). – If the shared secret is configured, verify that you have the same shared secret entered on the authentication server. – If the shared secret is not configured, enter it, and ensure that it matches the one on the authentication server.
802.1X Not Enabled	
Phone cannot obtain a DHCP-assigned IP address Phone does not register with Cisco Unified Communications Manager Phone status display as "Configuring IP" or "Registering" 802.1X Authentication Status displays as "Disabled" Status menu displays DHCP status as timing out	These errors typically indicate that 802.1X authentication is not enabled on the phone. To enable it, see the "802.1X Authentication and Status" section on page 4-31.

Table 9-1 Cisco Unified IP Phone Security Troubleshooting (continued)

Problem	Possible Cause
Factory Reset Deleted 802.1X Shared Secret	
Phone cannot obtain a DHCP-assigned IP address	These errors typically indicate that the phone has completed a factory reset (see the "Performing a Factory Reset" section on page 9-14) while 802.1X was enabled. A factory reset deletes the shared secret, which is required for 802.1X authentication and network access. To resolve this, you have two options: • Temporarily disable 802.1X authentication on the switch. • Temporarily move the phone to a network environment that is not using 802.1X authentication. Once the phone starts up normally in one of these conditions, you can access the 802.1X configuration menus and re-enter the shared secret (see the "802.1X Authentication and Status" section on page 4-31).
Phone does not register with Cisco Unified Communications Manager	
Phone status display as "Configuring IP" or "Registering"	
Cannot access phone menus to verify 802.1X status	

General Troubleshooting Tips

Table 9-2 provides general troubleshooting information for the Cisco Unified IP Phone.

Table 9-2 Cisco Unified IP Phone Troubleshooting

Summary	Explanation
Daisy-chaining IP phones	Cisco does not support connecting an IP phone to another IP phone through the PC port. Each IP phone should directly connect to a switch port. If phones are connected together in a line (by using the PC port), the phones will not work.
Poor quality when calling mobile phones using the G.729 protocol	In Cisco Unified Communications Manager, you can configure the network to use the G.729 protocol (the default is G.711). When using G.729, calls between an IP phone and a mobile phone will have poor voice quality. Use G.729 only when absolutely necessary.
Prolonged broadcast storms cause IP phones to reset, or be unable to make or answer a call	A prolonged Layer 2 broadcast storm (lasting several minutes) on the voice VLAN may cause IP phones to reset, lose an active call, or be unable to initiate or answer a call. Phones may not come up until a broadcast storm ends.

Table 9-2 Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
Moving a network connection from the phone to a workstation	If you are powering your phone through the network connection, you must be careful if you decide to unplug the phone's network connection and plug the cable into a desktop computer. **Caution** The computer's network card cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.
Changing the telephone configuration	By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See the "Unlocking and Locking Options" section on page 4-3 for details.
LCD display issues	If the display appears to have rolling lines or a wavy pattern, it might be interacting with certain types of older fluorescent lights in the building. Moving the phone away from the lights, or replacing the lights, should resolve the problem.
Dual-Tone Multi-Frequency (DTMF) delay	When you are on a call that requires keypad input, if you press the keys too quickly, some of them might not be recognized.
Codec mismatch between the phone and another device	The RxType and the TxType statistics show the codec that is being used for a conversation between this Cisco Unified IP phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation or that a transcoder is in place to handle the service. See the "Call Statistics Screen" section on page 7-13 for information about displaying these statistics.
Sound sample mismatch between the phone and another device	The RxSize and the TxSize statistics show the size of the voice packets that are being used in a conversation between this Cisco Unified IP phone and the other device. The values of these statistics should match. See the "Call Statistics Screen" section on page 7-13 for information about displaying these statistics.
Gaps in voice calls	Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics might indicate a problem with jitter on the network or periodic high rates of network activity. See the "Call Statistics Screen" section on page 7-13 for information about displaying these statistics.

Table 9-2 Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
Loopback condition	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option in the Network Configuration menu on the phone is set to **10 Half** (10-BaseT/half duplex) • The phone receives power from an external power supply • The phone is powered down (the power supply is disconnected) In this case, the switch port on the phone can become disabled and the following message will appear in the switch console log: HALF_DUX_COLLISION_EXCEED_THRESHOLD To resolve this problem, re-enable the port from the switch.
One-way audio	When at least one person in a call does not receive audio, IP connectivity between phones is not established. Check the configurations in routers and switches to ensure that IP connectivity is properly configures.
Peer to peer image distribution fails.	If the peer to peer image distribution fails, the phone will default to using the TFTP server to download firmware. Access the log messages stored on the remote logging machine to help debug the peer to peer image distribution feature. **Note** These log messages are different than the log messages sent to the phone log.
Cisco VT Advantage/ Unified Video Advantage (CVTA)	If you are having problems getting CVTA to work, make sure that the PC Port is enabled, and that CDP is enabled on the PC port.

General Troubleshooting Tips for the Cisco Unified IP Phone Expansion Module 7914

Table 9-3 provides general troubleshooting information for the Cisco Unified IP Phone Expansion Module 7914.

Table 9-3 Cisco Unified IP Phone Expansion Module 7914 Troubleshooting

Problem	Solution
No display on the Cisco Unified IP Phone Expansion Module 7914.	Verify that all of the cable connections are correct. Verify that you have power to the Cisco Unified IP Phone Expansion Module 7914.

Table 9-3 Cisco Unified IP Phone Expansion Module 7914 Troubleshooting (continued)

Problem	Solution
Lighted buttons on the first Cisco Unified IP Phone Expansion Module 7914 are all red.	Verify that the Cisco Unified IP Phone Expansion Module 7914 is configured in Cisco Unified Communications Manager.
Lighted buttons on the second Cisco Unified IP Phone Expansion Module 7914 are all amber.	Verify that the Cisco Unified IP Phone Expansion Module 7914 is configured in Cisco Unified Communications Manager.

Resetting or Restoring the Cisco Unified IP Phone

There are two methods for resetting or restoring the Cisco Unified IP Phone:

- Performing a Basic Reset, page 9-13
- Performing a Factory Reset, page 9-14

Performing a Basic Reset

Performing a basic reset of a Cisco Unified IP Phone provides a way to recover if the phone experiences an error and provides a way to reset or restore various configuration and security settings.

Table 9-4 describes the ways to perform a basic reset. You can reset a phone with any of these operations any time after the phone has started up. Choose the operation that is appropriate for your situation.

Table 9-4 Basic Reset Methods

Operation	Performing	Explanation
Restart phone	From the Main screen, press **Settings** to display the Settings menu, then press **#**. **Note** This factory reset sequence also works from any other screen that does not accept user input.	Resets any user and network configuration changes that you have made but that the phone has not written to its flash memory to previously saved settings, then restarts the phone.
Erase softkey	From the Settings menu, unlock phone options (see the "Unlocking and Locking Options" section on page 4-3). Then press the **Erase** softkey.	Resets user and network configuration settings to their default values, deletes the CTL file from the phone, and restarts the phone.
	From the Network Configuration menu, unlock phone options (see the "Unlocking and Locking Options" section on page 4-3). The press the **Erase** softkey.	Resets network configuration settings to their default values and resets the phone. (This method causes DHCP reconfigure the IP address of the phone.)
	From the Security Configuration menu, unlock phone options (see the "Unlocking and Locking Options" section on page 4-3). Then press the **Erase** softkey.	Deletes the CTL file from the phone and restarts the phone.

Performing a Factory Reset

When you perform a factory reset of the Cisco Unified IP Phone, the following information is erased or reset to its default value:

- CTL file—Erased
- LSC—Erased
- User configuration settings—Reset to default values
- Network configuration settings—Reset to default values
- Call histories—Erased
- Locale information—Reset to default values
- Phone application—Erased (phone recovers by loading the term70.default.loads file or the term71.default.loads file, depending on the phone model)

Before you perform a factory reset, ensure that the following conditions are met:

- The phone must be on a DHCP-enabled network.
- A valid TFTP server must be set in DHCP option 150 or option 66 on the DHCP server.
- The term70.default.loads file or the term71.default.loads file and the files specified in that file should be available on the TFTP server that is specified by the DHCP packet.

To perform a factory reset of a phone, perform the following steps:

Procedure

Step 1 Unplug the power cable from the phone and then plug it back in.

The phone begins its power-up cycle.

Step 2 While the phone is powering up, and before the Speaker button flashes on and off, press and hold **#**.

Continue to hold # until each line button flashes on and off in sequence in orange.

Step 3 Release **#** and press **123456789*0#**.

You can press a key twice in a row, but if you press the keys out of sequence, the factory reset will not take place.

After you press these keys, the line buttons on the phone flash orange and then green, and the phone goes through the factory reset process. This process can take several minutes.

Do not power down the phone until it completes the factory reset process, and the main screen displays.

Using the Quality Report Tool

The Quality Report Tool (QRT) is a voice quality and general problem-reporting tool for the Cisco Unified IP Phone. The QRT feature is installed as part of the Cisco Unified Communications Manager installation.

You can configure users' Cisco Unified IP Phones with QRT. When you do so, users can report problems with phone calls by pressing the **QRT** softkey. This softkey is available only when the Cisco Unified IP Phone is in the Connected, Connected Conference, Connected Transfer, and/or OnHook states.

When a user presses the **QRT** softkey, a list of problem categories appears. The user selects the appropriate problem category, and this feedback is logged in an XML file. Actual information logged depends on the user selection and whether the destination device is a Cisco Unified IP Phone.

For more information about using QRT, refer to *Cisco Unified Communications Manager Features and Services Guide*.

Monitoring the Voice Quality of Calls

To measure the voice quality of calls that are sent and received within the network, Cisco Unified IP Phones use these statistical metrics that are based on concealment events. The DSP plays concealment frames to mask frame loss in the voice packet stream.

- Concealment Ratio metrics—Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.
- Concealed Second metrics—Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely "concealed second" is a second in which the DSP plays more than five percent concealment frames.
- MOS-LQK metrics—Use a numeric score to estimate the relative voice listening quality. The Cisco Unified IP Phone calculates the mean opinion score (MOS) for listening quality (LQK) based audible concealment events due to frame loss in the preceding 8 seconds, and includes perceptual weighting factors such as codec type and frame size.

  MOS LQK scores are produced by a Cisco proprietary algorithm, Cisco Voice Transmission Quality (CVTQ) index. Depending on the MOS LQK version number, these scores might be compliant with the International Telecommunications Union (ITU) standard P.564. This standard defines evaluation methods and performance accuracy targets that predict listening quality scores based on observation of actual network impairment.

Note Concealment ratio and concealment seconds are primary measurements based on frame loss while MOS LQK scores project a "human-weighted" version of the same information on a scale from 5 (excellent) to 1 (bad) for measuring listening quality.

Listening quality scores (MOS LQK) relate to the clarity or sound of the received voice signal. Conversational quality scores (MOS CQ such as G.107) include impairment factors, such as delay, that degrade the natural flow of conversation.

You can access voice quality metrics from the Cisco Unified IP Phone by using the Call Statistics screen (see the "Call Statistics Screen" section on page 7-13) or remotely by using Streaming Statistics (see the "Monitoring the Cisco Unified IP Phone Remotely" chapter).

Using Voice Quality Metrics

To use the metrics for monitoring voice quality, note the typical scores under normal conditions of zero packet loss and use the metrics as a baseline for comparison.

It is important to distinguish significant changes from random changes in metrics. Significant changes are scores that change about 0.2 MOS or greater and persist in calls that last longer than 30 seconds. Conceal Ratio changes should indicate greater than 3 percent frame loss.

MOS LQK scores can vary based on the codec that the Cisco Unified IP Phone uses. The following codecs provide these maximum MOS LQK scores under normal conditions with zero frame loss:

- G.711 codec gives 4.5 score
- G.729A/ AB gives 3.7

Note

- CVTQ does not support wideband (7 kHz) speech codecs, as ITU has not defined the extension of the technique to wideband. Therefore, MOS scores that correspond to G.711 performance are reported for G.722 calls to allow basic quality monitoring, rather than not reporting an MOS score.
- Reporting G.711-scale MOS scores for wideband calls through the use of CVTQ allows basic quality classifications to be indicated as good/normal or bad/abnormal. Calls with high scores (approximately 4.5) indicate high quality/low packet loss, and lower scores (approximately 3.5) indicate low quality/high packet loss.
- Unlike MOS, the Conceal Ratio and Concealed Seconds metrics remain valid and useful for both wideband and narrowband calls.

A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

Troubleshooting Tips

When you observe significant and persistent changes to metrics, use Table 9-5 for general troubleshooting information:

Table 9-5 Changes to Voice Quality Metrics

Metric Change	Condition
MOS LQK scores decrease significantly	Network impairment from packet loss or high jitter: • Average MOS LQK decreases could indicate widespread and uniform impairment. • Individual MOS LQK decreases indicate bursty impairment. Cross-check with Conceal Ratio and Conceal Seconds for evidence of packet loss and jitter.
MOS LQK scores decrease significantly	• Check to see if the phone is using a different codec than expected (RxType and TxType). • Check to see if the MOS LQK version changed after a firmware upgrade.

Table 9-5 Changes to Voice Quality Metrics

Metric Change	Condition
Conceal Ratio and Conceal Seconds increase significantly	• Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	• Noise or distortion in the audio channel such as echo or audio levels. • Tandem calls that undergo multiple encode/decode such as calls to a mobile network or calling card network. • Acoustic problems coming from a speakerphone, handsfree mobile phone or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.

Note Voice quality metrics do not account for noise or distortion, only frame loss.

Where to Go for More Troubleshooting Information

If you have additional questions about troubleshooting the Cisco Unified IP Phones, several Cisco.com web sites can provide you with more tips. Choose from the sites available for your access level.

- Cisco Unified IP Phone Troubleshooting Resources:

  http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

- Cisco Products and Services (Technical Support and Documentation):

  http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

Cleaning the Cisco Unified IP Phone

To clean your Cisco Unified IP phone, use a soft, dry cloth to wipe the phone and the touchscreen. Do not apply liquids or powders directly on the phone. As with all non-weather-proof electronics, liquids and powders can damage the components and cause failures.

Disable the touchscreen before cleaning it so that you will not inadvertently choose a feature from the pressure of the cleaning cloth. To disable the touchscreen so that it will not respond to touch, press the **Display** button for more than one second. The phone displays Touchscreen Disabled and the **Display** button flashes green.

After one minute, the touchscreen automatically re-enables itself. To re-enable the touchscreen before that, press the flashing **Display** button for more than one second. The phone displays Touchscreen Enabled.

APPENDIX A

Providing Information to Users Via a Website

If you are a system administrator, you are likely the primary source of information for Cisco Unified IP Phone users in your network or company. It is important to provide current and thorough information to end users.

Cisco recommends that you create a web page on your internal support site that provides end users with important information about their Cisco Unified IP Phones.

Consider including the following types of information on this site:

- How Users Obtain Support for the Cisco Unified IP Phone, page A-1
- Giving Users Access to the User Options Web Pages, page A-1
- How Users Access the Online Help System on the Phone, page A-2
- How Users Get Copies of Cisco Unified IP Phone Manuals, page A-2
- Accessing Cisco 7900 Series Unified IP Phone eLearning Tutorials (SCCP Phones Only), page A-2
- How Users Subscribe to Services and Configure Phone Features, page A-3
- How Users Access a Voice-Messaging System, page A-3
- How Users Configure Personal Directory Entries, page A-4

How Users Obtain Support for the Cisco Unified IP Phone

To successfully use some of the features on the Cisco Unified IP Phone (including speed dial, services, and voice-messaging system options), users must receive information from you or from your network team or be able to contact you for assistance. Make sure to provide end users with the names of people to contact for assistance and with instructions for contacting those people.

Giving Users Access to the User Options Web Pages

Before a user can access the User Options web pages, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager end user group: choose **User Management > User Groups**. For additional information, refer to:

- *Cisco Unified Communications Manager Administration Guide*, “User Group Configuration” chapter
- *Cisco Unified Communications Manager System Guide*, “Roles and User Groups” chapter

How Users Access the Online Help System on the Phone

This Cisco Unified IP Phone 7970 Series provides access to a comprehensive online help system. To view the main help menu on a phone, press the **?** button on the phone. If you are already in Help, press **Main**.

Main menu topics include:

- About Your Cisco Unified IP Phone—Descriptive information about the phone model
- How do I...?—Procedures and information about commonly used phone tasks
- Calling Features—Descriptions and procedures for using calling features, such as conference and transfer
- Help—Tips on using and accessing Help

You can also use the **?** button to obtain information about softkeys, menu items, and the help system itself. Refer to *Cisco Unified IP Phone 7970 Series Guide* for more information.

How Users Get Copies of Cisco Unified IP Phone Manuals

You should provide end users with access to user documentation for the Cisco Unified IP Phones. *Cisco Unified IP Phone 7970 Series Guide* includes detailed user instructions for key phone features.

There are several Cisco Unified IP Phone models available, so to assist users in finding the appropriate documentation on the Cisco website, Cisco recommends that you provide links to the current documentation. If you do not want to or cannot send users to the Cisco website, Cisco suggests that you download the PDF files and provide them to end users on your website.

For a list of available documentation, go to the Cisco Unified IP Phone website at this URL:

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

For more information about viewing or ordering documentation, see the "Document Conventions" section on page xiii.

Additionally, you can provide end users with access to self-paced Cisco Unified IP Phone eLearning tutorials for several phone models. The tutorials can include a link to a user guide PDF. For more information, see the "Accessing Cisco 7900 Series Unified IP Phone eLearning Tutorials (SCCP Phones Only)" section on page A-2.

Accessing Cisco 7900 Series Unified IP Phone eLearning Tutorials (SCCP Phones Only)

Cisco 7900 Series Unified IP Phone eLearning tutorials use audio and animation to demonstrate basic calling features for SCCP phones. The eLearning tutorials are currently available for the Cisco Unified IP Phone 7970 Series (7970G/7971G-GE), and the Cisco Unified IP Phone models 7961G/G-GE, 7941G/G-GE, 7960G, 7940G, 7912G, and 7905G.

End-users can access runtime versions of the eLearning tutorials (English only) from Cisco.com by looking for tutorials under relevant phone models at this site:

http://cisco.com/en/US/products/hw/phones/ps379/products_user_guide_list.html

Administrators can download customizable versions of the eLearning tutorials (English only) from the phone product pages on Cisco.com at

http://cisco.com/en/US/products/hw/phones/ps379/prod_models_home.html

Refer to the tutorial Read Me file that is included with the relevant eLearning tutorial for specific instructions, including how to link to the most recent user guide PDF.

Note The eLearning tutorials are updated periodically and therefore might not contain the latest feature information for end-users. For the latest feature information, end-users should refer to the Cisco Unified IP Phone end-user documentation specific to their phone model and Cisco Unified Communications Manager version.

How Users Subscribe to Services and Configure Phone Features

End users can perform a variety of activities by using the Cisco Unified Communications Manager User Options web pages. These activities include subscribing to services, setting up speed dial and call forwarding numbers, configuring ring settings, and creating a personal address book. Keep in mind that configuring settings on a phone by using a website might be new for your end users. You need to provide as much information as possible to ensure that they can successfully access and use the User Options web pages.

Make sure to provide end users with the following information about the User Options web pages:

- The URL required to access the application. This URL is:

  https://*servername*:portnumber/ccmuser, where *server_name* is the host on which the web server is installed.

- A user ID and default password are needed to access the application.

  These settings correspond to the values you entered when you added the user to Cisco Unified Communications Manager (see the "Adding Users to Cisco Unified Communications Manager" section on page 5-20).

- A brief description of what a web-based, graphical user interface application is, and how to access it with a web browser.

- An overview of the tasks that users can accomplish using the web page.

You can also refer users to *Cisco Unified IP Phone 7970 Series Guide*, which is available at this URL:

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

How Users Access a Voice-Messaging System

Cisco Unified Communications Manager lets you integrate with many different voice mail messaging systems, including the Cisco Unity voice-messaging system. Because you can integrate with a variety of systems, you must provide users with information about how to use your specific system.

You should provide this information to each user:

- How to access the voice mail messaging system account.

  Make sure that you have used Cisco Unified Communications Manager to configure the **Messages** button on the Cisco Unified IP Phone.

- Initial password for accessing the voice messaging system.

  Make sure that you have configured a default voice messaging system password for all users.

- How the phone indicates that voice messages are waiting.

  Make sure that you have used Cisco Unified Communications Manager to set up a message waiting indicator (MWI) method.

How Users Configure Personal Directory Entries

Users can configure personal directory entries on the Cisco Unified IP Phone. To configure a personal directory, users must have access to the following:

- User Options web pages—Make sure that users know how to access their User Options web pages. See the "How Users Subscribe to Services and Configure Phone Features" section on page A-3 for details.
- Cisco Unified IP Phone Address Book Synchronizer—Make sure to provide users with the installer for this application. To obtain the installer, choose **Application > Plugins** from Cisco Unified Communications Manager Administration and click **Download**, which is located next to the **Cisco Unified IP Phone Address Book Synchronizer** plugin name. When the file download dialog box displays, click **Save**. Send the TabSyncInstall.exe file to all users who require this application.

See the "Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer" section on page A-4 for information about installing the Cisco Unified IP Phone Address Book Synchronizer.

Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer

Use this tool to synchronize data stored in your Microsoft Windows address book with the Cisco Unified Communications Manager directory and the User Options Personal Address Book.

Tip To successfully synchronize the Windows address book with the Personal Address Book, all Windows address book users should be entered in the Windows address book before performing the following procedures.

Installing the Synchronizer

Step 1 Get the Cisco Unified IP Phone Address Book Synchronizer installer file from your system administrator.

Step 2 Double-click the TabSyncInstall.exe file provided by your system administrator.

The publisher dialog box displays.

Step 3 Click **Run**.

The Welcome to the InstallShield Wizard for Cisco Unified CallManager Personal Address Book Synchronizer window displays.

Step 4 Click **Next**.

The License Agreement window displays.

Step 5 Read the license agreement information, and click the **I Accept** radio button. Click **Next**.

The Destination Location window displays.

Step 6 Choose the directory in which you want to install the application and click **Next**.

The Ready to Install window displays.

Step 7 Click **Install**.

The installation wizard installs the application to your computer. When the installation is complete, the InstallShield Wizard Complete window displays.

Step 8 Click **Finish**.

Step 9 To complete the process, follow the steps in the "Configuring the Synchronizer" section on page A-5.

Configuring the Synchronizer

Step 1 Open the Cisco Unified IP Phone Address Book Synchronizer.

If you accepted the default installation directory, you can open the application by choosing **Start > All Programs > Cisco Systems > TabSync**.

Step 2 To configure user information, click the **User** button.

The Cisco Unified CallManager User Information window displays.

Step 3 Enter the Cisco Unified IP Phone user name and password and click **OK**.

Step 4 To configure Cisco Unified Communications Manager server information, click the **Server** button.

The Configure Cisco Unified CallManager Server Information window displays.

Step 5 Enter the IP address or host name and the port number of the Cisco Unified Communications Manager server and click **OK**.

If you do not have this information, contact your system administrator.

Step 6 To start the directory synchronization process, click the **Synchronize** button.

The Synchronization Status window provides information on the status of the address book synchronization. If you chose the user intervention for duplicate entries rule and you have duplicate address book entries, the Duplicate Selection window displays. Choose the entry that you want to include in your Personal Address Book and click **OK**.

When synchronization completes, click **Exit** to close the Cisco Unified CallManager Address Book Synchronizer. To verify if the synchronization worked, log in to your User Options web pages and choose Personal Address Book. The users from your Windows address book should be listed.

APPENDIX B

Feature Support by Protocol for the Cisco Unified IP Phones 7970 Series

This appendix provides information about feature support for the Cisco Unified IP Phones 7970 Series using the SCCP or SIP protocol with Cisco Unified Communications Manager Release 7.0.

Table B-1 provides a high-level overview of calling features and their support by protocol. This table focuses primarily on end-user calling features and is not intended to represent a comprehensive listing of all available phone features.

Table B-1 also provides references to appropriate sections in *Cisco Unified IP Phone 7970G/7971G-GE User Guide for Cisco Unified Communications Manager 7.0*, which is available at this URL:

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

Table B-1 Cisco Unified IP Phone 7970G/7971G-GE Feature Support by Protocol

Features	Cisco Unified IP Phone 7970G/7971G-GE		For More Information
	SCCP	SIP	
Calling Features			
Abbreviated Dialing	Supported	Supported	"Basic Call Handling—Placing a Call: Additional Options"
Anonymous Call Block	Not supported	Supported	
Audible Message Waiting Indicator	Supported	Supported	"Accessing Voice Messages"
Auto Answer	Supported	Supported	"Using a Handset, Headset, and Speakerphone—Using Auto Answer"
Auto-pickup	Supported	Supported	
Auto Dial	Supported	Supported	"Basic Call Handling—Placing a Call: Basic Options"
Barge (and cBarge)	Supported	Supported	"Advanced Call Handling—Using a Shared Line"
Block external to external transfer	Supported	Supported	
Busy Lamp Field (BLF)	Supported	Supported	"Advanced Call Handling—Using BLF to Determine a Line State"
Busy Lamp Field (BLF) Pickup	Supported	Supported	"Advanced Call Handling—Using BLF to Determine a Line State"

Table B-1 Cisco Unified IP Phone 7970G/7971G-GE Feature Support by Protocol (continued)

Features	Cisco Unified IP Phone 7970G/7971G-GE		For More Information
	SCCP	SIP	
Calling Features			
Call Back	Supported	Supported	"Basic Call Handling—Placing a Call: Additional Options"
Call Display Restrictions	Supported	Supported	
Call Forward All	Supported	Supported	"Basic Call Handling—Forwarding Calls to Another Number"
Call Forward All Breakout	Supported	Supported	
Call Forward All Loop Prevention	Supported	Supported	
Call Forward Busy	Supported	Supported	"Basic Call Handling—Forwarding Calls to Another Number"
Call Forward Configurable Display	Supported	Supported	
Call Forward Destination Override	Supported	Supported	
Call Forward No Answer	Supported	Supported	"Basic Call Handling—Forwarding Calls to Another Number"
Call Park	Supported	Supported	"Advanced Call Handling—Storing and Receiving Parked Calls"
Call Pickup/Group Call Pickup/Directed Call Pickup	Supported	Supported	"Advanced Call Handling—Picking Up a Redirected Call on Your Phone"
Call Recording	Supported	Supported	
Call Waiting	Supported	Supported	"Basic Call Handling—Answering a Call"
Caller ID	Supported	Supported	"An Overview of Your Phone—Understanding Touch Screen Features" or "An Overview of Your Phone—Understanding Phone Screen Features"
Caller ID Blocking	Supported	Supported	
Call Back	Supported	Supported	
Cisco Unified Communications Manager Assistant	Supported	Supported	
Client Matter Codes (CMC)	Supported	Not supported	"Basic Call Handling—Placing a Call: Additional Options"
Computer Telephony Integration (CTI) Applications	Supported	Some support (such as Call Park, WMI)	Users do not interact with this feature directly. It is configured on Cisco Unified Communications Manager.
Configurable Call Forward Display	Supported	Supported	
Direct Transfer	Supported	Not supported	

Table B-1 Cisco Unified IP Phone 7970G/7971G-GE Feature Support by Protocol (continued)

Features	Cisco Unified IP Phone 7970G/7971G-GE		For More Information
	SCCP	SIP	
Calling Features			
Directed Call Park	Supported	Supported	"Advanced Call Handling—Storing and Receiving Parked Calls"
Do Not Disturb (DND)	Supported	Supported	"Basic Call Handling—Using Do Not Disturb"
Distinctive Ring	Supported	Supported	"Using Phone Settings—Customizing Rings and Message Indicators"
Extension Mobility Service	Supported	Supported	"Advanced Call Handling—Using Cisco Extension Mobility"
Fast Dial Service	Supported	Supported	"Advanced Call Handling—Speed Dialing"
Forced Authorization Codes (FAC)	Supported	Not supported	"Basic Call Handling—Placing a Call: Additional Options"
Group Call Pickup	Supported	Supported	
Help System	Supported	Supported	"An Overview of Your Phone—Understanding Feature Buttons and Menus"
Hold/Resume	Supported	Supported	"Basic Call Handling—Using Hold and Resume"
Hold Reversion	Supported	Supported	"Basic Call Handling—Using Hold and Resume"
Hunt Group	Supported	Supported	
Immediate Divert	Supported	Supported	"Basic Call Handling—Answering a Call"
Immediate Divert—Enhanced	Supported	Supported	"Basic Call Handling—Sending a Call to a Voice Messaging System"
Intercom	Supported	Supported	"Basic Call Handling—Placing or Receiving Intercom Calls"
Join/Select	Supported	Supported	"Basic Call Handling—Making Conference Calls"
Join Across Lines/Select	Supported	Supported	"Basic Call Handling—Making Conference Calls"
Log Out of Hunt Groups	Supported	Supported	"Advanced Call Handling—Logging Out of Hunt Groups"
Malicious Call ID	Supported	Supported	"Advanced Call Handling—Tracing Suspicious Calls"
Meet-Me Conference	Supported	Supported	"Basic Call Handling—Making Conference Calls"
Message Waiting Indicator	Supported	Supported	
Mobile Connect	Supported	Supported	
Mobile Voice Access	Supported	Supported	
Multilevel Precedence and Preemption (MLPP)	Supported	Not supported	"Advanced Call Handling—Prioritizing Critical Calls"
Multiple Calls per Line Appearance	200	50	"An Overview of Your Phone—Understanding Lines vs. Calls"
Music-on-Hold	Supported	Supported	
Mute	Supported	Supported	"Basic Call Handling—Using Mute"

Table B-1 Cisco Unified IP Phone 7970G/7971G-GE Feature Support by Protocol (continued)

Features	Cisco Unified IP Phone 7970G/7971G-GE		For More Information
	SCCP	SIP	
Calling Features			
On-hook Dialing/Pre-Dial	Supported	Supported	"Basic Call Handling—Placing a Call: Basic Options"
Onhook Call Transfer	Supported	Supported	
Other Group Pickup	Supported	Supported	
Presence-Enabled Directories	Supported	Supported	
Privacy	Supported	Supported	"Advanced Call Handling—Using a Shared Line"
Private Line Automated Ringdown (PLAR)	Supported	Supported	
Programmable Line Keys	Supported	Supported	Feature descriptions throughout phone guide
Protected Calling	Supported	Supported	"An Overview of the Cisco Unified IP Phone—Understanding Security Features for Cisco Unified IP Phones"
Quality Reporting Tool (QRT)	Supported	Supported	"Troubleshooting—Using the Quality Reporting Tool"
Redial	Supported	Supported	"Basic Call Handling—Placing a Call: Basic Options"
Ring Setting	Supported	Supported	
Secure Conference	Supported	Supported	"Basic Call Handling—Making Conference Calls"
Services	Supported	Supported	
Services URL button	Supported	Supported	
Shared Line	Supported	Supported	"Advanced Call Handling—Using a Shared Line"
Silent Monitoring	Supported	Supported	
Single Button Barge	Supported	Supported	"Advanced Call-Handling—Using Barge to Add Yourself to a Shared-Line Call"
Speed Dialing	Supported	Supported	"Advanced Call Handling—Speed Dialing"
Time-of-Day Routing	Supported	Supported	
Touchscreen Illumination Disabling	Supported	Supported	
Transfer	Supported	Supported	"Basic Call Handling—Transferring Calls"
Transfer - Direct Transfer	Supported	Not supported	"Basic Call Handling—Transferring Calls"
URL Dialing	Not supported	Supported	"Using Call Logs and Directories—Using Call Logs"
Video Mode	Supported	Not supported	
Video Support	Supported	Not supported	"Understanding Additional Configuration Options"
Voice Mail	Supported	Supported	"Accessing Voice Messages" section of the Phone Guide

Table B-1 Cisco Unified IP Phone 7970G/7971G-GE Feature Support by Protocol (continued)

Features	Cisco Unified IP Phone 7970G/7971G-GE		For More Information
	SCCP	SIP	
Calling Features			
WebDialer	Supported	Supported	"Customizing Your Phone on the Web—Configuring Features and Services on the Web"
Settings			
Call Statistics	Supported	Supported	"Troubleshooting Your Phone—Viewing Phone Administrative Data"
Voice Quality Metrics	Supported	Supported	"Troubleshooting Your Phone—Viewing Phone Administrative Data"
Services			
SDK Compliance	4.0(1)	4.0(1)	*Cisco Unified IP Phone Service Application Development Notes for Release 4.1(3)* or later
Directories			
Call Logs	Supported	Supported	"Using Call Logs and Directories—Directory Dialing"
Corporate Directories	Supported	Supported	"Using Call Logs and Directories—Directory Dialing"
Personal Directory Enhancements	Supported	Supported	"Using Call Logs and Directories—Directory Dialing"
Supplemental Features and Applications			
Cisco Unified Communications Manager Assistant	Supported	Supported	*Cisco Unified Communications Manager Assistant User Guide*
Cisco Communications Manager AutoAttendant	Supported	Supported	*Cisco Unified Communications Manager Features and Services Guide*
Cisco Unified Communications Manager Attendant Console	Supported	Supported	*Cisco Unified Communications Manager Attendant Console User Guide*
Cisco Unified IP Phone Expansion Module 7914	Supported	Supported	*Cisco Unified IP Phone Expansion Module 7914 Guide*
Cisco VT Advantage	Supported	Not supported	*Cisco VT Advantage User Guide*

APPENDIX C

Supporting International Users

Translated and localized versions of the Cisco Unified IP Phones are available in several languages. If you are supporting Cisco Unified IP Phones in a non-English environment, refer to the following sections to ensure that the phones are set up properly for your users:

- Adding Language Overlays to Phone Buttons, page C-1
- Installing the Cisco Unified Communications Manager Locale Installer, page C-1
- Support for International Call Logging, page C-2

Adding Language Overlays to Phone Buttons

To support the needs of international users, the button labels on the Cisco Unified IP Phones exhibit icons rather than text to indicate the purposes of the buttons. You can purchase language-specific text overlays to add to a phone. To order these language-specific overlays, go to this website:

http://www.overlaypro.com/cisco_systems?b=1

Note Phone overlays are available only for languages in which the Cisco Unified IP Phone software has been localized. All languages may not be immediately available, so continue to check the website for updates.

Installing the Cisco Unified Communications Manager Locale Installer

If you are using Cisco Unified IP Phones in a locale other than English (United States), you must install the locale-specific version of the Cisco Unified Communications Manager Locale Installer on every Cisco Unified Communications Manager server in the cluster. Installing the locale installer ensures that you have the latest translated text, user and network locales, and country-specific phone tones available for the Cisco Unified IP Phones. You can find locale-specific versions of the Cisco Unified Communications Manager Locale Installer at http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml.

For more information, refer to the “Locale Installation” section in the *Cisco Unified Communications Platform Administration Guide.*

Note All languages may not be immediately available, so continue to check the website for updates.

Support for International Call Logging

If your phone system is configured for international call logging, the call logs, redial, or call directory entries may display a “+” symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the “+” may be replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the “+” with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes.

APPENDIX D

Technical Specifications

The following sections describe the technical specifications for the Cisco Unified IP Phone 7970 Series.

- Physical and Operating Environment Specifications, page D-1
- Cable Specifications, page D-2
- Network and Access Port Pinouts, page D-2

Physical and Operating Environment Specifications

Table D-1 shows the physical and operating environment specifications for the Cisco Unified IP Phone.

Table D-1 Physical and Operating Specifications

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 95% (non-condensing)
Storage temperature	14° to 140°F (–10° to 60°C)
Height	9.07 in. (23.03 cm)
Width	10.5 in. (26.67 cm)
Depth	• 2.54 in. (6.45 cm)—with footstand fully closed • 6.0 in. (15.24 cm)—with footstand fully open
Weight	3.25 lb (1.47 kg)
Power options	• The phone can receive power from IEEE 802.3af-compliant data switches (Class III) • The phone can be powered locally with a power adapter (Cisco part number CP-PWR-CUBE-3=) and the appropriate power cord (power requirements for the power adapter: 100-240 VAC, 50-60 Hz, 0.5 A)

Table D-1 Physical and Operating Specifications (continued)

Specification	Value or Range
Cables	Category 3/5/5e for 10-Mbps cables with 4 pairs Category 5/5e for 100-Mbps cables with 4 pairs Category 5e/6 for 1000-Mbps cables with 4 pairs **Note** Cables have 4 pairs of wires for a total of 8 conductors.
Distance requirements	As supported by the Ethernet specification, it is assumed that the maximum cable length between each Cisco Unified IP Phone and the switch is 100 meters (330 feet).

Cable Specifications

- RJ-9 jack (4-conductor) for handset and headset connection.
- RJ-45 jack for the LAN 10/100/1000BaseT connection (labeled 10/100/1000 SW).
- RJ-45 jack for a second 10/100/1000BaseT compliant connection (labeled 10/100/1000 PC).
- 3.5 mm jack for microphone and speaker connection.
- 48-volt power connector.

Network and Access Port Pinouts

Although both the network and access ports are used for network connectivity, they serve different purposes and have different port pinouts.

Network Port Connector

Table D-2 describes the network port connector pinouts.

Table D-2 Network Port Connector Pinouts

Pin Number	Function
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	5BI_DC-
6	6BI_DB-
7	7BI_DD+
8	BI_DD-

Note "BI" stands for bi-directional, while DA, DB, DC and DD stand for "Data A", "Data B", "Data C" and "Data D", respectively.

Access Port Connector

Table D-3 describes the access port connector pinouts.

Table D-3 Access Port Connector Pinouts

Pin Number	Function
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	5BI_DD-
6	6BI_DA-
7	7BI_DC+
8	BI_DC-

Note "BI" stands for bi-directional, while DA, DB, DC and DD stand for "Data A", "Data B", "Data C" and "Data D", respectively.

APPENDIX E

Basic Phone Administration Steps

This appendix provides minimum, basic configuration steps for you to do the following:

- Add a new user to Cisco Unified Communications Manager Administration
- Configure a new phone for that user
- Associate that user to that phone
- Complete other basic end-user configuration tasks

The procedures provide one method for performing these tasks and are not the only way to perform these tasks. They are a streamlined approach to get a new user and corresponding phone running on the system.

These procedures are designed to be used on a mature Cisco Unified Communications Manager system where calling search spaces, partitions, and other complicated configuration have already been done and are in place for existing users.

This section contains these topics:

- Example User Information for these Procedures, page E-1
- Adding a User to Cisco Unified Communications Manager, page E-2
- Configuring the Phone, page E-3
- Performing Final End User Configuration Steps, page E-7

Example User Information for these Procedures

In the procedures that follow, examples are given when possible to illustrate some of the steps. Sample user and phone information used throughout these procedures includes:

- User's Name: John Doe
- User ID: johndoe
- Phone model: 7961G
- Protocol: SCCP
- MAC address listed on phone: 00127F576611
- Five-digit internal telephone number: 26640

Adding a User to Cisco Unified Communications Manager

This section describes steps for adding a user to Cisco Unified Communications Manager. Follow one of the procedures in this section, depending on your operating system and the manner in which you are adding the user:

- Adding a User From an External LDAP Directory, page E-2
- Adding a User Directly to Cisco Unified Communications Manager, page E-2

Adding a User From an External LDAP Directory

If you added a user to an LDAP Directory (a non-Cisco Unified Communications Server directory), you can immediately synchronize that directory to the Cisco Unified Communications Manager on which you are adding this same user and the user's phone by following these steps:

Procedure

Step 1 Log onto Cisco Unified Communications Manager Administration.

Step 2 Choose **System > LDAP > LDAP Directory**.

Step 3 Use the **Find** button to locate your LDAP directory.

Step 4 Click on the LDAP directory name.

Step 5 Click **Perform Full Sync Now**.

Note If you do not need to immediately synchronize the LDAP Directory to the Cisco Unified Communications Manager, the LDAP Directory Synchronization Schedule on the LDAP Directory window determines when the next auto-synchronization is scheduled. However, the synchronization must occur before you can associate a new user to a device.

Step 6 Proceed to Configuring the Phone, page E-3.

Adding a User Directly to Cisco Unified Communications Manager

If you are not using an LDAP directory, you can add a user directly to Cisco Unified Communications Manager Administration by following these steps:

Procedure

Step 1 Choose **User Management > End User**, then click **Add New.** The End User Configuration window appears.

Step 2 In the User Information pane of this window, enter the following:

- User ID—Enter the end user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.

  Example: *johndoe*

- Password and Confirm Password—Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.

- Last Name—Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.)

  Example: *doe*

- Telephone Number—Enter the primary directory number for the end user. End users can have multiple lines on their phones.

  Example: 26640 (John Doe’s internal company telephone number)

Step 3 Click **Save**.

Step 4 Proceed to the section Configuring the Phone, page E-3.

Configuring the Phone

First, perform the following procedure to identify the user’s phone model and protocol:

Procedure

Step 1 From Cisco Unified Communications Manager administration, choose **Device > Phone >.**

Step 2 Click **Add New**.

Step 3 Select the user’s phone model from the Phone Type drop-down list, then click **Next**.

Step 4 Select the device protocol (SCCP or SIP) from the drop-down list, then click **Next**. The Phone Configuration window appears.

Procedure

On the Phone Configuration window, you can use the default values for most of the fields.

Step 1 For the required fields, possible values, some of which are based on the example of user *johndoe*, can be configured as follows:

a. In the Device Information pane of this window:

- MAC Address—Enter the MAC address of the phone, which is listed on a sticker on the phone.

Make sure that the value comprises 12 hexadecimal characters.

Example: 00127F576611 (MAC address on john doe's phone)

- Description—This is an optional field in which you can enter a useful description, such as *john doe's phone*. This will help you if you need to search on information about this user.
- Device Pool—Choose the device pool to which you want this phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.

Note Device Pools are defined on the Device Pool Configuration window of Cisco Unified Communications Server Administration (**System > Device Pool**).

- Phone Button Template—Choose the appropriate phone button template from the drop-down list. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.

Note Phone button templates are defined on the Phone Button Template Configuration window of Cisco Unified Communications Manager Administration (**Device > Device Settings > Phone Button Template**). You can use the search field(s) in conjunction with the **Find** button to find all configured phone button templates and their current settings.

- Softkey Template—Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. Leave this field blank if the common device configuration contains the assigned softkey template.

Note Softkey templates are defined on the Softkey Template Configuration window of Cisco Unified Communications Manager Administration (**Device > Device Settings > Softkey Template**). You can use the search field(s) in conjunction with the **Find** button to find all configured softkey templates and their current settings.

- Common Phone Profile—From the drop-down list box, choose a common phone profile from the list of available common phone profiles.

Note Common Phone Profiles are defined on the Common Phone Profile Configuration window of Cisco Unified Communications Manager Administration (**Device > Device Settings > Common Phone Profile**). You can use the search field(s) in conjunction with the **Find** button to find all configured common phone profiles and their current settings.

- Calling Search Space—From the drop-down list box, choose the appropriate calling search space (CSS). A calling search space comprises a collection of partitions (analogous to a collection of available phone books) that are searched to determine how a dialed number should be routed. The calling search space for the device and the calling search space for the directory number get used together. The directory number CSS takes precedence over the device CSS.

Note Calling Search Spaces are defined on the Calling Search Space Configuration window of Cisco Unified Communications Manager Administration (**Calling routing > Class of Control> Calling Search Space**). You can use the search field(s) in conjunction with the **Find** button to find all configured Calling Search Spaces and their current settings.

- Location—Choose the appropriate location for this Cisco Unified IP Phone.
- Owner User ID—From the drop-down menu, choose the user ID of the assigned phone user.

b. In the Protocol Specific Information pane of this window, choose a Device Security Profile from the drop-down list. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. If the phone does not support security, choose a non-secure profile.

To identify the settings that are contained in the profile, choose **System > Security Profile > Phone Security Profile**.

Note The security profile chosen should be based on the overall security strategy of the company.

c. (For SIP Phones only) Also in the Protocol Specific Information pane of this window, choose the applicable SIP Profile from the drop-down list.

d. In the Extension Information pane of this window, check the Enable Extension Mobility box if this phone supports Cisco Extension Mobility.

e. In the Product Specific Configuration Layout pane of this window, enable the Video Capabilities field if this field appears on your window.

f. Click **Save**.

Step 2 Configure line settings:

a. On the Phone Configuration window, click Line 1 on the left pane of the window. The Directory Number Configuration window appears.

b. In the Directory Number field, enter a valid number that can be dialed.

Note This field should contain the same number that appears in the Telephone Number field on the User Configuration window.

Example: 26640 is the directory number of user John Doe in the example above.

c. From the Route Partition drop-down list, choose the partition to which the directory number belongs. If you do not want to restrict access to the directory number, choose <None> for the partition.

d. From the Calling Search Space drop-down list (Directory Number Settings pane of the Directory Number Configuration window), choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that are using this directory number.

e. In the Call Pickup and Call Forward Settings pane of the Directory Number Configuration window, choose the items (i.e. Forward All, Forward Busy Internal) and corresponding destinations to which calls should be sent.

   Example: If you want incoming internal and external calls that receive a busy signal to be forwarded to the voice mail for this line, check the Voice Mail box next to the "Forward Busy Internal" and "Forward Busy External" items in the left column of the Call Pickup and Call Forward Settings pane.

f. In the "Line 1 on Device..." pane of the Directory Number Configuration window, configure the following:

   - Display (Internal Caller ID field)—You can enter the first name and last name of the user of this device so that this name will be displayed for all internal calls. You can also leave this field blank to have the system display the phone extension.
   - External Phone Number Mask—Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line.

     You can enter a maximum of 24 number and "X" characters. The Xs represent the directory number and must appear at the end of the pattern.

     Example: Using the john doe extension in the example above, if you specify a mask of 408902XXXX, an external call from extension 6640 displays a caller ID number of 4089026640.

   Note This setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the **Propagate Selected** button. (The check box at right displays only if other devices share this directory number.)

g. Click **Save**.

h. Click **Associate End Users** at the bottom of the window to associate a user to the line being configured. Use the Find button in conjunction with the Search fields to locate the user, then check the box next to the user's name, then click **Add Selected**. The user's name and user ID should now appear in the "Users Associated With Line" pane of the Directory Number Configuration window.

i. Click **Save**. The user is now associated with Line 1 on the phone.

j. If your phone has a second line, configure Line 2.

k. Associate the user with the device:

   - Choose **User Management > End User**.
   - Use the search boxes and the Find button to locate the user you have added (i.e. *doe* for the last name).
   - Click on the user ID (i.e. *johndoe*). The End User Configuration window appears.
   - Click **Device Associations**.
   - Use the Search fields and the Find button to locate the device with which you want to associate to the user. Select the device, then click **Save Selected/Changes**. The user is now associated with the device.
   - Click the **Go** button next to the "Back to User" Related link in the upper-right corner of the screen.

l. Proceed to Performing Final End User Configuration Steps, page E-7.

Performing Final End User Configuration Steps

If you are not already on the End User Configuration page, choose **User Management > End User** to perform some final configuration tasks. Use the Search fields and the Find button to locate the user (i.e. John Doe), then click on the user ID to get to the End User Configuration window for the user.

In the End User configuration window, do the following:

Procedure

Step 1 In the Directory Number Associations pane of the screen, set the primary extension from the drop-down list.

Step 2 In the Mobility Information pane, check the Enable Mobility box.

Step 3 In the Permissions Information pane, use the User Group buttons to add this user to any user groups. For example, you may want to add the user to a group that has been defined as a "Standard CCM End User Group."

To view all configured user groups, choose **User Management > User Group**.

Step 4 Click **Save**.

INDEX

Symbols

"more" Softkey Timer 4-18

.cnf.xml configuration file 2-7

Numerics

10/100/1000 PC port 3-2

See also access port

10/100/1000 SW port 3-2

See also network port

10/100 PC port 3-2

See also access port

10/100 SW port 3-2

See also network port

802.1X

authentication server 1-17

authenticator 1-17

description 1-4

network components 1-16

supplicant 1-17

Troubleshooting 9-9, 9-10

802.1X Authentication 4-30

802.1X authentication and status 4-31

802.1X Authentication menu

options 4-32

Device Authentication 4-32

EAP-MD5 4-32

802.1X Authentication Status menu

about 4-30

states 4-33

A

abbreviated dialing 5-2, B-1

AC adapter, connecting 3-5

access, to phone settings 3-12, 4-2

access port

10/100/1000 PC 3-2

10/100 PC 3-2

configuring 4-7

connecting 3-5

disabled 4-24

forwarding packets to 4-23

access to phone settings 4-1

Access web page 8-2, 8-8

adding

Cisco Unified IP Phones manually 2-12

Cisco Unified IP Phones using auto-registration 2-10

Cisco Unified IP Phones using BAT 2-12

users to Cisco Unified Communications Manager 5-20

adjusting, phone placement of 3-8

adjustment plate 3-10

Admin. VLAN ID 4-6

Advance Adhoc Conference service parameter 5-7

Alternate TFTP 4-9

anonymous call block 5-2, B-1

answer release B-2, B-3

Audible message waiting indicator 5-2, B-1

audience, for this document ii-xi

authenticated call 1-13

authentication 1-9, 3-12

authentication server, in 802.1X 1-17

Authentication URL 4-16

authenticator, in 802.1X 1-17
auto answer 5-2, B-1
Auto Call Select 4-18
auto dial 5-2, B-1
Auto Line Select 4-17
auto-pickup 5-2, B-1
auto-registration
  using 2-10
auxiliary VLAN 2-3

B

background image
  configuring 6-5
  creating 6-3
  custom 6-3
  List.xml file 6-4
  PNG file 6-4, 6-5
barge 1-17, 5-3, B-1
BAT (Bulk Administration Tool) 2-12
block external to external transfer 5-3, B-1
BootP 1-4
BOOTP Server 4-10
Bootstrap Protocol (BootP) 1-4
Busy Lamp Field (BLF) 5-3, B-1
  call lists 4-17
  pickup 5-3, B-1

C

cable lock, connecting to phone 3-8
call
  authenticated 1-13
  encrypted 1-13
  protected 1-13
  security interactions 1-15
Call Back 5-3, B-2
call back B-2
call display restrictions 5-4, B-2
caller ID 5-5, B-2
Caller ID Blocking 5-6
caller ID blocking B-2
call forward
  all breakout B-2
  all calls 5-4, B-2
  all loop prevention B-2
  busy B-2
  configurable display B-2
  destination override 5-4
  display, configuring 5-4
  loop breakout 5-4
  loop prevention 5-4
  no answer B-2
call forward display, configuring 5-4, 5-7
call park 5-5, B-2
call pickup 5-5, B-2
Call Preferences menu 4-14
call recording 5-5
Call Statistics screen 7-1, 7-13
call waiting 5-5, B-2
CAPF (Certificate Authority Proxy Function) 1-11, 3-12
certificate trust list file
  See CTL file
Cisco Discovery Protocol
  See CDP
Cisco Peer to Peer Distribution Protocol (CPPDP) 1-4
Cisco Unified Communications Manager
  adding phone to database of 2-9
  interactions with 2-2
  required for Cisco Unified IP Phones 3-2
  verifying settings 9-4
Cisco Unified Communications Manager Administration
  adding telephony features using 5-1
  configuring LCD display using 6-8
Cisco Unified Communications Manager Assistant 5-6, B-2

Cisco Unified IP Phone
adding manually to Cisco Unified Communications Manager 2-12
adding to Cisco Unified Communications Manager 2-9
cleaning 9-17
configuration checklist 1-19
configuration requirements 1-18
configuring user services 5-20
features 1-1
figure 1-1
installation checklist 1-21
installation overview 1-18
installation procedure 3-5
installation requirements 1-18
modifying phone button templates 5-17
mounting to wall 3-9
power sources 2-3
registering 2-9
registering with Cisco Unified Communications Manager 2-10, 2-12
resetting 9-13
supported networking protocols 1-3
technical specifications D-1
troubleshooting 9-1
using LDAP directories 5-17
web page 8-1
Cisco Unified IP Phone Expansion Module 7914
statistics 7-3, 7-12
troubleshooting 9-12
cleaning the Cisco Unified IP Phone 9-17
Clear softkey 7-4, 7-9
client matter codes 5-6, B-2
computer telephony integration (CTI) 5-6, B-2
conference 5-7
secure 1-14
See secure conference
conference joining 5-7
configurable call forward display 5-7, B-2
configuration file
.cnf.xml 2-7
creating 9-5
encrypted 1-12
modifying 6-1
overview 2-6
secure 2-6
XmlDefault.cnf.xml 2-7
configuring
from a Cisco Unified IP Phone 4-3
LDAP directories 5-17
overview 1-18
personal directories 5-17
phone button templates 5-17
softkey templates 5-19
startup network settings 3-11
user features 5-20
connecting
handset 3-5
headset 3-5
to AC adapter 3-5
to a computer 3-5
to the network 3-5
Console Logs web page 8-2
Core Dumps web page 8-2
CTL file
deleting from phone 9-13
requesting 2-8
CTL File menu 4-30
CTL File screen 4-30
custom phone rings
about 6-2
creating 6-2, 6-3, 6-5
PCM file requirements 6-3

D

daisy chaining 9-10
data VLAN 2-3

Days Display Not Active 4-22, 6-8
Debug Display web page 8-2, 8-10
Default Router 1-5 4-8
Device Authentication 4-32
device authentication 1-11
Device Configuration menu
displaying 4-2
editing values 4-3
overview 4-1
sub-menus 4-10
Device Information web page 8-2, 8-3
DHCP 4-8
description 1-4
troubleshooting 9-7
DHCP Address Released 4-9
DHCP Server 4-8
directed call park 5-7, B-3
directed call pickup 5-7
directories button 1-3
Directories URL 4-15
directory numbers, assigning manually 2-12
direct transfer 5-7, B-2
display, turning on and off automatically 6-8
Display button 6-8, 9-17
display button 1-2
Display Idle Timeout 4-22, 6-9
Display On Duration 4-22, 6-8
Display On Time 4-22, 6-8
Display On When Incoming Call 6-9
Display On When Incoming call 4-22
distinctive ring 5-7, B-3
DND 5-8, B-3
DNS server
troubleshooting 9-7
verifying settings 9-4
DNS Server 1-5 4-8
documentation
additional ii-xii
for users A-2
Domain Name 4-6
Domain Name System (DNS) 4-6
Domain Name System (DNS) server 4-8
do not disturb 5-8
DSCP For Call Control 4-25
DSCP For Configuration 4-25
DSCP For Services 4-25
Dynamic Host Configuration Protocol
See DHCP

E

EAP-MD5 4-32
Device ID 4-32
Realm 4-32
Shared Secret 4-32
editing, configuration values 4-3
encrypted call 1-13
encrypted configuration file 1-12
encryption
media 1-9, 1-11
signaling 1-9, 1-11
Erase softkey 9-13
error messages, used for troubleshooting 9-3
Ethernet Configuration menu
about 4-23
Span to PC Port option 4-23
Ethernet Information web page 8-2, 8-8
Expansion Module
See Cisco Unified IP Phone Expansion Module 7914
Expansion Module(s) screen 7-3, 7-12
extension mobility 5-8, B-3

F

fast dial service 5-8, B-3

feature buttons
directories 1-3
help 1-3
messages 1-2
services 1-3
settings 1-3
features
configuring on phone, overview 1-8
configuring with Cisco Unified Communications Manager, overview 1-8
informing users about 1-8
support by protocol
abbreviated dialing B-1
anonymous call block B-1
answer release B-2, B-3, B-4
Audible message waiting indicator B-1
auto answer B-1
auto dial B-1
auto-pickup B-1
barge B-1
block external to external transfer B-1
Busy Lamp Field (BLF) B-1
pickup B-1
Call Back B-2
call back B-2
call display restrictions B-2
caller ID B-2
caller ID blocking B-2
call forward
all breakout B-2
all calls B-2
all loop prevention B-2
busy B-2
configurable display B-2
no answer B-2
call park B-2
call pickup B-2
call waiting B-2
Cisco Unified Communications Manager Assistant B-2
client matter codes B-2
computer telephony integration (CTI) Applications B-2
configurable call forward display B-2
directed call park B-3
direct transfer B-2
distinctive ring B-3
DND B-3
extension mobility B-3
fast dial service B-3
forced authorization codes B-3
group call pickup B-3
Help system B-3
hold B-3
hold reversion B-3
hunt group B-3
immediate divert B-3
Immediate divert enhanced B-3
intercom B-3
join B-3
join across lines B-3
log out of hunt groups B-3
malicious caller identification (MCID) B-3
meet-me conference B-3
message waiting B-3
mobile connect B-3
mobile voice access B-3
multilevel precedence and preemption (MLPP) B-3
music-on-hold B-3
mute B-3
onhook call transfer B-4
on-hook dialing B-4
other group pickup B-4
presence-enabled directories B-4
privacy B-4
Private Line Automated Ringdown (PLAR) B-4
programmable line keys B-4
protected calling B-4

Quality Reporting Tool (QRT) B-4
redial B-4
ring setting B-4
secure conference B-4
Services URL button B-4
shared line B-4
silent monitoring B-4
single button barge B-4
speed dialing B-4
Time-of-Day Routing B-4
touchscreen illumination disabling B-4
transfer B-4
transfer-direct transfer B-4
URL dialing B-4
video mode B-4
video support B-4
voice mail B-4
web dialer B-5
figure
Cisco Unified IP Phone features 1-1
Cisco Unified IP Phone rear cable connections 3-6
Cisco Unified IP Phone wall mount 3-10
file authentication 1-11
file format
List.xml 6-4
RingList.xml 6-2
firmware, verifying version 7-11
Firmware Versions screen 7-11
footstand
adjusting 3-8
adjustment button 1-2, 3-10
adjustment plate 3-10
identifying 1-2
forced authorization codes 5-9, B-3

G

G.722 codec 4-22
G.729 1-1
G.729a 1-1
G.729ab 1-1
G.729b 1-1
GARP Enabled 4-24
group call pickup 5-9, B-3

H

handset 1-3
handset, connecting 3-5
headset
audio quality 3-4
connecting 3-4
disabling 3-4
quality 3-4
sound quality 3-4
using 3-3
Headset button 1-3
Headset Enabled 4-19
headset port 3-5
height, adjusting 3-8
help button 1-3
Help system B-3
help system 5-9
hold 5-9, B-3
hold reversion 5-9, B-3
hookswitch clip, removing 3-3
Host Name 4-6
HTTP, description 1-4
HTTP Configuration menu
about 4-15
options
Authentication URL 4-16
Directories URL 4-15
Idle URL 4-16
Idle URL Time 4-16
Information URL 4-15
Messages URL 4-15
Proxy Server URL 4-16

Services URL 4-15
hunt group 5-9, B-3
log out of hunt groups 5-10
Hypertext Transfer Protocol
See HTTP

I

icon
lock 1-13
padlock 1-13
shield 1-13
idle display
configuring 6-7
timeout 4-16
viewing settings 6-7
XML service 4-16, 6-7
Idle URL 4-16
Idle URL Time 4-16
image authentication 1-11
immediate divert 5-9, B-3
Immediate divert enhanced 5-10, B-3
Information URL 4-15
installing
Cisco Unified Communications Manager configuration 3-2
network requirements 3-1
preparing 2-9
procedure 3-5
requirements, overview 1-18
intercom 5-10, B-3
interference, mobile phone 1-1
International Call Logging C-2
Internet Protocol (IP) 1-5
IP Address 4-8
IP address, troubleshooting 9-3
IPv4 Configuration 4-6
IPv6 Configuration 4-6

J

join 5-10, B-3
join across lines 5-10, B-3

K

keypad 1-3

L

language overlays C-1
LCD screen
disabling 9-17
turning on and off automatically 6-7
LDAP directories, using with Cisco Unified IP Phone 5-17
light strip, on handset 1-3
line buttons 1-2
Line Settings menu 4-14
Link Layer Discovery Protocol (LLDP)
network configuration 8-7
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)
network configuration 8-7
List.xml file 6-4
Locale Configuration menu
about 4-16, 4-17
options
Network Locale 4-16
Network Locale Version 4-17
User Locale 4-16
User Locale Char Set 4-16
User Locale Version 4-16
Locale Installer C-1
localization
Installing the Cisco Unified Communications Manager Locale Installer C-1
phone button overlays for C-1

Locally Significant Certificate (LSC) 3-12
lock icon 1-13
Logging Display 4-24
log out of hunt groups B-3
Log server 4-27

M

MAC address 4-6
malicious caller identification (MCID) 5-11, B-3
manufacturing installed certificate (MIC) 1-11
Media Configuration menu
  about 4-19
  options
    Headset Enabled 4-19
    Recording Tone 4-20
    Recording Tone Duration 4-21
    Recording Tone Local Volume 4-20
    Recording Tone Remote Volume 4-20
    Speaker Enabled 4-19
    Video Capability Enabled 4-19
media encryption 1-11
meet-me conference 5-11, B-3
messages button 1-2
Messages URL 4-15
message waiting 5-11, B-3
metrics, voice quality 8-11
MIC 1-11
mobile connect 5-11, B-3
mobile phone interference 1-1
mobile voice access 5-11, B-3
Model Information screen 7-1
multilevel precedence and preemption (MLPP) 5-11, B-3
multiple calls per line appearance 5-11
music-on-hold 5-12, B-3
mute
  button 1-3
  feature 5-12, B-3

N

native VLAN 2-3
navigation button 1-3
Network Configuration Area items
  LLDP-MED on SW port 8-7
  LLDP on PC port 8-7
Network Configuration menu 4-25
  about 4-5
  displaying 4-2
  editing values 4-3
  IPv4
    options
      Alternate TFTP 4-9
      BOOTP Server 4-10
      Default Router 1-5 4-8
      DHCP 4-8
      DHCP Address Released 4-9
      DHCP Server 4-8
      DNS Server 1-5 4-8
      IP Address 4-8
      Subnet Mask 4-8
      TFTP Server 1 4-9
  locking options 4-3
  options
    Admin. VLAN ID 4-6
    CDP on PC port 4-27
    CDP on switch port 4-28
    Domain Name 4-6
    Host Name 4-6
    IPv4
      TFTP Server 2 4-10
    MAC Address 4-6
    Operational VLAN ID 4-6
    PC Port Configuration 4-7
    PC VLAN 4-7
    SW Port Configuration 4-7
  overview 4-1
  unlocking options 4-3
Network Configuration web page 8-2, 8-4

network connectivity, verifying 9-3
networking protocol
802.1X 1-4
BootP 1-4
CDP 1-4
CPPDP 1-4
DHCP 1-4
HTTP 1-4
IP 1-5
RTCP 1-5
RTP 1-5
SCCP 1-6
SIP 1-6
TCP 1-6
TFTP 1-6
TLS 1-6
UDP 1-6
networking protocols, supported 1-3
Network Locale 4-16
Network Locale Version 4-17
network outages, identifying 9-6
network port
10/100/1000 SW 3-2
10/100 SW 3-2
configuring 4-7
connecting to 3-5
network requirements, for installing 3-1
network settings, startup configuration 3-11
network statistics 7-9, 8-8
Network Statistics screen 7-9
Network web page 8-2, 8-8

O

onhook call transfer 5-12, B-4
on-hook dialing B-4
onhook predialing 5-12
Operational VLAN ID 4-6
other group pickup 5-12, B-4

P

padlock icon 1-13, 4-3
PC, connecting to the phone 3-3
PCM file requirements, for custom ring types 6-3
PC Port Configuration 4-7
PC Port Disabled 4-24
PC VLAN 4-7
Peer firmware sharing 4-27
personal directories 5-17
phone button templates, modifying 5-17
phone lines, buttons for 1-2
phone screen 2-5
phone settings access 4-1
physical connection, verifying 9-6
plugging in Cisco Unified IP Phone 3-5
PNG file 6-4, 6-5
power
maximum required from a switch 2-5
providing to the Cisco Unified IP Phone 2-3
power consumption 2-5
Power over Ethernet (PoE) 2-3
Power Save Configuration menu
about 4-22
options
Days Display Not Active 4-22
Display Idle Timeout 4-22
Display On Duration 4-22
Display On Time 4-22
Display On When Incoming call 4-22
power source
causing phone to reset 9-8
description 2-3
effect on phone screen brightness 2-5
external power 2-3, 2-4
PoE 2-3, 2-4
power consumption 2-5
power injector 2-4
presence-enabled directories 5-12, B-4

privacy 5-12, B-4
Private Line Automated Ringdown (PLAR) 5-12, B-4
programmable buttons, description 1-2
programmable line keys 5-13, B-4
protected call 1-13
description 1-14
protected calling
all calls B-4
description 5-13
Protected Calls 1-14
Proxy Server URL 4-16

Q

QoS Configuration menu
about 4-25
options
DSCP For Call Control 4-25
DSCP For Configuration 4-25
DSCP For Services 4-25
QRT softkey 5-13, 9-15
Quality Reporting Tool (QRT) 5-13, 9-14, B-4

R

Real-Time Control Protocol
See RTCP
Real-Time Transport Protocol
See RTP
Recording Tone 4-20
Recording Tone Duration 4-21
Recording Tone Local Volume 4-20
Recording Tone Remote Volume 4-20
redial 5-13, B-4
reset
basic 9-13
factory 9-14
resetting
basic 9-13
Cisco Unified IP phone 9-13
continuously 9-6
intentionally 9-7
methods 9-13
ring activity 5-13
ringer, indicator for 1-3
RingList.xml file format 6-2
ring setting B-4

S

SCCP, description 1-6
screen
See LCD screen
secure conference B-4
description 1-14, 5-14
establishing 1-14
identifying 1-14
restrictions 1-15
secure SRST reference 1-11
securing the phone with a cable lock 3-8
security
CAPF (Certificate Authority Proxy Function) 1-11, 3-12
configuring on phone 3-12
device authentication 1-11
encrypted configuration file 1-12
file authentication 1-11
image authentication 1-11
Locally Significant Certificate (LSC) 3-12
manufacturing installed certificate (MIC) 1-11
media encryption 1-11
secure configuration file 2-6
secure SRST reference 1-11
security profiles 1-12
signaling authentication 1-11
signaling encryption 1-11

Security Configuration menu (on Device Configuration menu)
about 4-23
options
GARP Enabled 4-24
Logging Display 4-24
PC Port Disabled 4-24
Security Mode 4-24
Voice VLAN Enabled 4-24
Web Access Enabled 4-24
Security Configuration menu (on Settings menu)
about 4-29
options
802.1X Authentication 4-30
802.1X Authentication Status 4-30
CAPF Server 4-29
CTL File 4-29
LSC 4-29
MIC 4-29
Security Mode 4-29
Trust List 4-29
Web Access Enabled 4-29
Security Mode 4-24
security profiles 1-12
services
configuring for users 5-20
description 5-14
protocol support B-4
subscribing to 5-20
services button 1-3
Services URL 4-15
Services URL button 5-14, B-4
settings button 1-3
Settings menu access 3-12, 4-2
shared line 5-14, B-4
shield icon 1-13
signaling authentication 1-11
signaling encryption 1-11
silent monitoring 5-14, B-4
single button barge 5-15, B-4
SIP, description 1-6
SIP Configuration menu 4-12
SIP General Configuration menu 4-13
softkey buttons, description 1-3
softkey templates, configuring 5-19
Span to PC Port 4-23
Speaker button
description 1-3
disabling 3-3
Speaker Enabled 4-19
speakerphone, button for 1-3
speed dial
buttons for 1-2
template for 5-18
speed dialing 5-2, 5-14, 5-15, B-4
SRST 8-5
description 4-12
secure reference 1-11
standard (ad hoc) conference 5-7
startup problems 9-1
startup process
accessing TFTP server 2-8
configuring VLAN 2-8
contacting Cisco Unified Communications Manager 2-9
loading stored phone image 2-7
obtaining IP address 2-8
obtaining power 2-7
requesting configuration file 2-9
requesting CTL file 2-8
understanding 2-7
verifying 3-10
statistics
call 7-13
network 7-9, 8-8
streaming 8-10
Status menu
description 7-1

submenus on 7-3
status messages 7-3
Status Messages screen 7-3
Status Messages web page 8-2, 8-10
Stream 0 web page 8-10
Stream 1 web page 8-2, 8-10
Stream 2 web page 8-2, 8-10
Stream 3 web page 8-2, 8-10
streaming statistics 8-10
Subnet Mask 4-8
supplicant, in 802.1X 1-17
Survivable Remote Site Telephony
See SRST
SW Port Configuration 4-7

T

TCP 1-6
technical specifications, for Cisco Unified IP Phone D-1
telephony features
abbreviated dialing 5-2
anonymous call block 5-2
Audible message waiting indicator 5-2
auto answer 5-2
auto dial 5-2
auto-pickup 5-2
barge 1-17, 5-3
block external to external transfer 5-3
Busy Lamp Field (BLF) 5-3
Busy Lamp Field (BLF) pickup 5-3
Call Back 5-3
call display restrictions 5-4
caller ID 5-5
caller ID blocking 5-6
call forward 5-4
call forward configurable display 5-4
call park 5-5
call pickup 5-5
call recording 5-5
call waiting 5-5
Cisco Unified Communications Manager Assistant 5-6
client matter codes 5-6
computer telephony integration (CTI) 5-6
conference 5-7
configurable call forward display 5-7
directed call park 5-7
directed call pickup 5-7
direct transfer 5-7
distinctive ring 5-7
extension mobility 5-8
fast dial service 5-8
forced authorization codes 5-9
group call pickup 5-9
help system 5-9
hold 5-9
hold reversion 5-9
hunt group 5-9
immediate divert 5-9
join 5-10
log out of hunt groups 5-10
Log server 4-27
malicious caller identification (MCID) 5-11
meet-me conference 5-11
mobile connect 5-11
mobile voice access 5-11
multilevel precedence and preemption (MLPP) 5-11
multiple calls per line appearance 5-11
music-on-hold 5-12
mute 5-12
no not disturb (DND) 5-8
onhook call transfer 5-12
onhook predialing 5-12
other group pickup 5-12
Peer firmware sharing 4-27
presence-enabled directories 5-12
privacy 5-12
programmable line keys 5-13

redial 5-13
ring activity 5-13
services 5-14
Services URL button 5-14
shared line 5-14
silent monitoring 5-14
speed dialing 5-15
Time-of-Day Routing 5-15
touchscreen illumination disabling 5-15
transfer 5-15
video mode 5-16
video support 5-16
voice messaging system 5-16
TFTP
description 1-6
troubleshooting 9-3
TFTP Server 1 4-9
TFTP Server 2 4-10
TFTP settings 1-9
time, displayed on phone 3-2
Time-of-Day Routing 5-15, B-4
TLS 2-6
touchscreen
cleaning 9-17
disabling 9-17
enabling 9-17
See also LCD screen
touchscreen illumination disabling 5-15, B-4
transfer 5-15, B-4
transfer-direct transfer B-4
Transmission Control Protocol
See TCP
Transport Layer Security
See TLS
Trivial File Transfer Protocol
See TFTP
troubleshooting
Cisco Unified Communications Manager settings 9-4
Cisco Unified IP Phone 9-1
Cisco Unified IP Phone Expansion Module 7914 9-12
DHCP 9-7
DNS 9-7
DNS settings 9-4
IP addressing and routing 9-3
network connectivity 9-3
network outages 9-6
phones resetting 9-7
physical connection 9-6
services on Cisco Unified Communications Manager 9-4
TFTP settings 9-3
VLAN configuration 9-7
Trust List menu 4-31

U

UI Configuration menu 4-17
options
Auto Call Select 4-18
Auto Line Select 4-17
BLF for call lists 4-17
uncompressed wideband 1-1
Unified CM Configuration 4-11
Unlock softkey 4-31
URL dialing B-4
User Datagram Protocol
See UDP
User Locale 4-16
User Locale Char Set 4-16
User Locale Version 4-16
User Options web page
description 5-21
giving users access to 5-21, A-1
specifying options that appear 5-21
users
adding to Cisco Unified Communications Manager 5-20
configuring personal directories A-4

documentation for A-2
providing required information to A-1
providing support to A-1
subscribing to services A-3

V

verifying
firmware version 7-11
startup process 3-10
Video Capability Enabled 4-19
video mode 5-16, B-4
video support 5-16, B-4
VLAN
auxiliary, for voice traffic 2-3
configuring 4-6
configuring for voice networks 2-3
native, for data traffic 2-3
verifying 9-7
voice mail B-4
voice messaging system 5-16
voice messaging system, accessing A-3
voice quality metrics 8-11
voice VLAN 2-3
Voice VLAN Enabled 4-24
volume button 1-3

W

wall mounting 3-9
Web Access Enabled 4-24
web dialer B-5
web page
about 8-1
Access 8-2, 8-8
accessing 8-1
Console Logs 8-2
Core Dumps 8-2
Debug Display 8-2, 8-10
Device Information 8-2, 8-3
disabling access to 8-3
Ethernet Information 8-2, 8-8
Network 8-2, 8-8
Network Configuration 8-4
Network Configuration web page 8-2
preventing access to 8-3
Status Messages 8-2, 8-10
Stream 0 8-10
Stream 1 8-2, 8-10
Stream 2 8-2, 8-10
Stream 3 8-2, 8-10
wideband handset 4-21
option 4-19
user controllable 4-19
wideband headset 4-21
option 4-18
user controllable 4-18

X

XmlDefault.cnf.xml 2-7